TALLINNA TEHNIKAÜLIKOOL
ELEKTROENERGEETIKA INSTITUUT

Centralized User Account Management Process in Substation Automation

Faculty of Power Engineering

Department of Electrical Power Engineering

Master of Science

Head of Chair	Juhan Valtin
Supervisors	Paul Taklaja
	Omar Velasco
Student	Kaspar Müül

Tallinn 2015

Declaration of authorship

I hereby declare that this thesis is the result of my own independent work and it has been presented to the department of Electrical Power Engineering of Tallinn University of Technology in order to claim a master's diploma in Electrical Power Engineering. This thesis has not been presented before to claim a degree in engineering sciences or engineering.

Student (date and signature) _____

Lõputöö kokkuvõte

Autor: Kaspar Müül *Lõputöö liik:* Magistritöö

Töö pealkiri: TSENTRALISEERITUD KASUTAJAKONTODE HALDAMISE PROTSESS ALAJAAMADE AUTOMAATIKA SÜSTEEMIDES

Kuupäev: 07.01.2015 *65 lk*

Ülikool: Tallinna Tehnikaülikool

Teaduskond: Energeetikateaduskond

Instituut: Elektroenergeetika instituut

Õppetool: Kõrgepingetehnika õppetool

Töö juhendajad: Paul Taklaja, Omar Velasco (ABB)

Töö konsultandid: Arve Sollie (ABB), Krister Hagman (ABB)

Sisu kirjeldus: Magistritöö kirjutamise tingis energiasektori vajadus töökindla ja turvalise tsentraaliseeritud kasutajakontode haldamise süsteemi järele, millega oleks võimalik hallata kasutajakontosid ning autentimist alajaamade automaatikasüsteemides kasutatavates intelligentsetes elektroonilistes seadmetes (IED-s). Käesoleva töö eesmärgiks on hinnata rakendatava tsentraliseeritud kasutajakontode haldamise süsteemi ja lahendada turvalisust puudutavad probleemid.

Töö sisaldab kokkuvõtet tsentraliseeritud autentimise vajaduse kujunemisest ja põhilistest süsteemi puudutavatest probleemidest. Magistritöö selguse huvides on üks peatükk pühendatud krüpteerimise ja avaliku võtme infrastruktuuri (PKI) tutvustamisele. Järgnevalt on tutvustatud rakendatavat tsentraliseeritud kasutajakontode haldamise süsteemi, mis põhineb LDAP protokollil, ning kirjeldatud ohte, mis töökindlust ja turvalisust võivad mõjutada. Tsentraliseeritud kasutajakontode haldamise süsteemi turvalisuse tõstmiseks on soovitatud andmevahetus krüpteerida. Erinevate osapoolte tuvastamiseks on soovitatud digitaalseid sertifikaate, mis on väljastatud tunnustatud kolmanda osapoole, sertifitseerimiskeskuse poolt. Lõpuks on lahendatud IED ja ühendatava kliendi platvormi vaheline tuvastusprobleem sertifikaatide määramisega ja andmevahetuse krüpteerimisega. Et IED-l oleks võimalik uus serveri sertifikaat väljastada kui interneti protokolli (IP) aadressi muudetakse, siis lahenduseks on toodud sertifitseerimiskeskuse (CA) salvestamine IED sisemisele mälule kuid salajane sertifitseerimiskeskuse signeerimisvõti turvalisuse tõstmiseks on salvestatud TPM turvakiibile. Krüpteerimisvõtmete turvaliseks salvestamiseks on soovitatud kasutada TPM turvakiipi.

Kokkuvõtteks, pakutav süsteem võimaldab võrgu omanikul hallata oma süsteemi kuuluvate IED-e kasutajaid lihtsamalt, kasutades tsentraalset süsteemi kasutajakonto lisamiseks, muutmiseks või kustutamiseks, vähendades süsteemi haldamisele kuluvat aega ja ressurssi. Lahendatud on turvalisust puudutavad probleemid, kaitstes andmevahetust ja autentides erinevaid osapooli ning lahendatud salajaste krüpteerimis võtmete turvalise salvestamise probleem TPM kiibi lisamisega IED emaplaadile.

Märksõnad: alajaamade turvalisus, automaatika, intelligentne elektrooniline seade (IED), krüptograafia, rollipõhine ligipääsu kontroll (RBAC), sertifitseerimiskeskus (CA), TPM turvakiip.

Summary of the diploma work

Author: Kaspar Müül *Type of work:* Master thesis

Title: CENTRALIZED USER ACCOUNT MANAGEMENT PROCESS IN SUBSTATION AUTOMATION

Date: 07.01.2015 *65 pages*

University: Tallinn University of Technology

Faculty: The faculty of Power Engineering

Department: The department of Electrical Power Engineering

Chair: The chair of High Voltage Engineering

Tutors: Paul Taklaja, Omar Velasco (ABB)

Consultants: Arve Sollie (ABB), Krister Hagman (ABB)

Abstract: The thesis in hand was motivated primarily because of the electrical industry's need for a reliable and secure centralized user account verification system that handles the user authentication process in Intelligent Electronic Devices (IEDs) in substation automation systems. The purpose of this study is to evaluate the proposed system, define the security status and propose solutions for security problems.

The work explains the need for a centralized authentication system, defines the problems with the existing solution and the proposed one. It includes a short introduction to cryptography. The thesis identifies the dangers of adding an authentication server, which is based on Lightweight Directory Access Protocol (LDAP), into a substation environment and analyzes the most common attacks a particular system may encounter. As a result of the study, in order to provide security in the network between two connecting entities, third party trusted certificates and encryption are recommended. During the analysis, two new obstacles were identified, and solutions were presented. First, when changes are done to the IED that affect the information in the Server Certificate (SC), a Certificate Authority (CA) should be installed onto the IED in order to create a new SC. Second, due to the unsecure nature of the internal storage options on the IED, a Trusted Platform Module (TPM) is recommended in order to safely secure the CAs signing private key, the symmetric key, and the asymmetric private key. Evaluation indicates that using digital certificates for identification and encryption to provide safety while the data is in transit or stored, can significantly improve the safety of the centralized user authentication system in the substation automation environment.

The proposed system has the ability to make the handling of user accounts in multiple IEDs easier by giving the responsible entity the possibility to modify, delete and add user information centrally, using a centralized server and interface, rather than modifying user accounts in each separate device. The security problems have been solved by using encryption while the data is in transit or stored, TPM chips will be used to safely store encryption keys, and digital certificates will be used for identification.

Key words: Certificate Authority (CA), cryptography, Intelligent Electronic Device (IED), Role Based Access Control (RBAC), substation security, automation, Transport Platform Module (TPM).

Contents

Assignment

Topic of thesis:	**Centralized User Account Management Process in Substation Automation**
Student:	**Kaspar Müül, 111324**
Supervisors:	**Paul Taklaja, Omar Velasco (ABB)**
Chair:	**High Voltage Engineering**
Head of chair:	**Juhan Valtin**
Due date for thesis:	**07 January 2015**

_____	_____	_____
Student (signature)	Supervisor (signature)	Head of chair (signature)

Justification of Topic

It is necessary to research this topic due to the increasing market demand for a reliable and secure centralized user account management system which can handle the administration of user accounts in a substation automation environment by giving the utility the possibility to change, add, delete, or modify user accounts in their Intelligent Electronic Devices (IEDs) centrally rather than modifying each device separately. Due to the standard requirements and customer focus on this topic, substation automation product manufacturers have started to look into this subject. The thesis in hand tries to answer and to give a proposal on how to improve the security between the IED and the centralized authentication server. It also focuses on the security and the authentication between the IED and the connecting client. Current IEDs lack the secure storage that is needed to store encryption keys safely, and this thesis gives a recommendation on the best solution for this particular problem.

This thesis may be of interest to anybody whose work or interest is related to substation security and critical infrastructure protection.

Purpose of Work

The purpose is to study the implications of adding a proposed system to a substation environment and develop a proposal to improve security.

List of Problems

- What dangers can arise when introducing a centralized authentication server into a substation environment?
- How to transfer user information over the network securely and to identify each entity?
- How to store encryption keys safely on the IED?

Initial Data

The data used in this work is obtained from IEC and NERC standards, from the ‘’Information Security Management Handbook’’ and relevant whitepapers.

Preface

This thesis is the result of the collaboration between ABB AB Substation Automation Products business unit located in Västerås, Sweden and myself, Kaspar Müül, during the fall of 2014.

I would like to thank my supervisors Omar Velasco, Krister Hagman and Arve Sollie from ABB for their continuous support while tackling this assignment. I would also like to thank my supervisor from the Tallinn University of Technology, Paul Taklaja, who supported the process from the beginning and helped me to edit the thesis.

I would like to thank the colleagues and personnel at ABB SA Products for a pleasant and supportive atmosphere. I am especially grateful to Mr. Kjell I. Westberg, manager of TPPA at ABB for organizing accommodation and everything else necessary for my stay in Sweden.

This research was supported by ABB and by the Estonian scholarship program Kristjan Jaak, which is funded and managed by Archimedes Foundation in collaboration with the Estonian Ministry of Education and Research.

Kaspar Müül

Abbreviations

CA- Certificate Authority

CC- Client Certificate

CCA- Critical Cyber Assets

CRL- Certificate Revocation List

DoS- Denial of Service

HMI- Human Machine Interface

IC- Integrated Circuit

I-CA- Intermediate Certificate Authority

IED- Intelligent Electronic Device

IP- Internet Protocol

LDAP- Lightweight Directory Access Protocol

OCSP- Online Certificate Status Protocol

PKI- Public Key Infrastructure

RAM- Random Access Memory

RBAC- Role Based Access Control

RBACMNT- Role-Based Access Control Manager

R-CA- Root Certificate Authority

SC- Server Certificate

S-CA- Subordinate Certificate Authority

SECADM- Security Administrator

SECAUD- Security Auditor

SPOF- Single Point of Failure

TLS- Transport Layer Security

TPM- Trusted Platform Module

VPN- Virtual Private Network

WAN- Wide Area Network

Introduction

Recent shifts in technology have created security problems as the electrical industry moved from closed proprietary networks to more standardized communication and protocols. The industry has benefitted from the operational side, because now it is easier to control its automation systems, but this has created several vulnerabilities and requires substation automation to address cyber-security issues that haven't been addressed in this industry before. This means that substation automation devices are getting connected to external networks where anyone with the knowledge and expertise can access them. As the energy grid is considered a critical infrastructure for a nation's well-being, focus is needed for access control. In most utilities and enterprises, network security and access control have already been implemented by the local IT department, and users have login access to their files, e-mails, and corporate networks. As the modern enterprise infrastructure has used centralized authentication for years, it's finally time to bring that knowledge down to the Intelligent Electronic Device (IED) level and implement similar control in substation environments.

The thesis in hand was motivated primarily because of the electrical industry's need for a reliable and secure centralized user account verification system that handles the user authentication process in IEDs. The proposed system has the ability to make the handling of user accounts in multiple IEDs easier by giving the responsible entity the possibility to modify, delete, and add user information centrally, using a centralized server and interface, rather than modifying user accounts in each separate device.

The advantage of centralized authentication is that the user list is managed in a single central location, by a responsible entity who, therefore, has full control over who can access its IEDs. There are still technical challenges extending that solution to the substation automation systems. Currently, IEC62351 standards define the need for a centralized user authentication system giving an overview on how it could be implemented and which models can be used, but it does not focus on the security between the IED and the connecting entity. Therefore to fill the gap and implement a fully controlled system more research is necessary. In order to implement a centralized authentication system, its safety and security requirements have to be analyzed. The purpose of this study is to evaluate the proposed system, define the security status, and propose solutions for security problems. This thesis is focused on the security between the authentication server and the IED and also between the client platform and the IED. The main task is to solve the authentication problem between devices in the network and to protect data while it is in

transit and when it is stored on the IED. One key question that the author hopes to answer is to find a secure storage option for encryption keys as the current IEDs lack that function. The goal is to propose a solution where every step is monitored and a fully controlled centralized user authentication process is achieved.

This thesis uses information from IEC62351 and NERC CIP standards. An important source for information has been the "Information Security Management Handbook'' [1] and relevant whitepapers, for example ''Making the most out of substation IEDs in a secure, NERC compliant manner'' [2], ''Efficient Public-Key Certificate Revocation Schemes for Smart Grid'' [3] and ''Best Practices in LDAP Security'' [4]. According to the author's findings, no specific research has been done on implementing secure storage on the IED level, the author hopes to fill the gap on this issue and to raise awareness on this possibility.

The first chapter explains the need for a centralized authentication system and explains Role-Based Access Control (RBAC) and the difference and problems with both decentralized and centralized authentication.

The second chapter is dedicated to explaining symmetric/asymmetric encryption, certificates, third party trust with Certificate Authorities (CAs) and the Transport Layer Security (TLS) in order to better understand the third and fourth chapter.

The third chapter is dedicated to the centralized user authentication management system, explaining Lightweight Directory Access Protocol (LDAP), and compares PUSH and PULL models. Based on the PULL model, a possible user authentication process is created between the authentication server and the IED. Possible failure modes and dangers are discussed including Single Point of Failure (SPOF), Denial of Service (DoS) and fake client/server situations. Possible solutions include encrypted connections to provide security for data while it is in transit, and for improved authentication, third party trusted certificates are recommended for each entity in the network.

The fourth chapter is dedicated to the security between the IED and the connecting client. Currently, there is no security for transferred data and authentication between the connecting client and the IED. Therefore, encryption during transit and certificates for each entity is recommended. In case the IEDs Internet Protocol (IP) address is changed a new Server Certificate (SC) is required. In order to get a new SC, it has to be manually installed on the IED or transferred over the network. In order to save resources, time and to improve security, a CA is installed on the IED so that the IED can create a new SC when needed. This created a problem

where the secret signing key can be stolen from the IEDs internal memory, so to avoid the secret key from being leaked, a secure storage option is recommended for storing encryption keys. A Trusted Platform Module (TPM) can provide the necessary security for storing the signing private key of the CA, the symmetric key, and the asymmetric private key on the IED. In order to handle certificates in the substation automation system, a possible combination of Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) has been introduced.

It must be noted that in this thesis, an IED is a protective relay. The centralized authentication server in this thesis is called the LDAP server. In most documents and standards SSL/TLS encryption is written together, but in this thesis, only the term TLS is used.

1 Access Control

1.1 Overview

Over the past decade, there has been a growing concern over the potential vulnerability of the electrical power grid to cyber-attacks. The industry operates as a whole to deliver electric power to its consumers in a reliable and secure way, when it stops, then so does everything else. Because utilities are required to provide a reliable stream of electric power, customers downstream from a substation rely heavily on its performance, therefore during abnormal operation, the customers are the ones who are most affected. Modern societies require a steady stream of electricity supply, and now this supply is getting computerized and connected creating new problems.

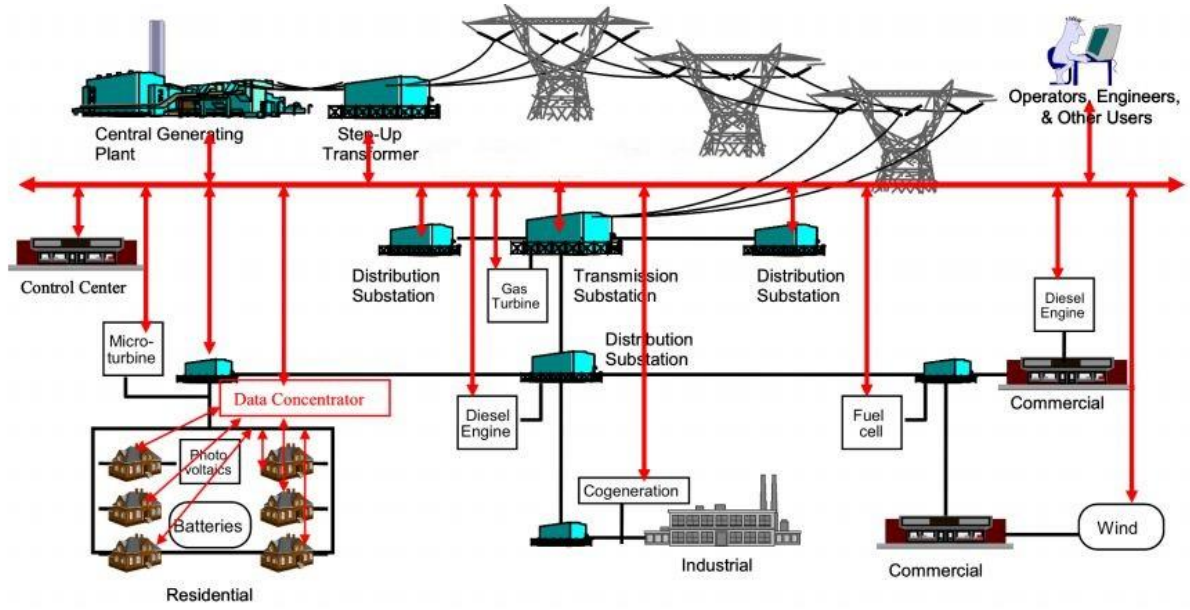

Figure 1.1.1 Power system infrastructure (black) and information infrastructure (red) [5]

Figure 1.1.1 shows that the power system infrastructure and information infrastructure has been fused together and combined in a way that they are now dependent on each other. This means that if the information infrastructure fails, then that will affect the power system infrastructure.

In the past, physical barriers like fences, walls, locked gates and doors were enough to keep unauthorized personnel from accessing the substations and other critically important facilities. Only people with the authorization were allowed to access the facility and had the entrance key to get into the territory, this strategy prevented mishaps caused by unapproved personnel. This was also the case for substation networks that have traditionally been isolated. Protocols, which were used to transfer information between devices, were often proprietary, meaning that they

were owned and used by a single organization. Security by obscurity was the main approach for decades as every vendor had their own communication protocol for their devices and these protocols were kept secret from the outside world. Often the messages sent between devices were in simple plaintext and no verification was done to check the message authenticity by the receiver. All of this has created security risks making the substation and its network more vulnerable to unauthorized access. [6] [7]

Only in the past decade have substation automation systems become more interconnected to provide a greater level of control [7]. Solutions based on open standards and commercial technologies have been made available to address the interoperability requirement between products made by different vendors. This has resulted in more standardized protocols for communication. Due to this requirement, substation networks can't rely anymore on security by isolation or on security by obscurity. Market focus for cyber security products has not been crucial until now as some incidents have gained public attention due to outbreaks of malware like Stuxnet that was designed to attack industrial control systems [1]. A single newspaper article explaining how a particular device has been compromised by malware can destroy the reputation and cause financial damage to the manufacturer of the product. This situation has created a need to invest into cyber-security.

The main reason to invest in security is to protect the organization not only from attacks by hackers and errors made by personnel, but also from the consequences following a breach or a malfunction that can result in a blackout leaving thousands of people and companies without electricity. A utility perhaps can regain its image in the public eye but a manufacturer of a product that was affected or was the cause of the breach due to the lack of security can destroy its image and reputation that took decades to build. It is therefore critical to invest into security and to keep developing and testing products for possible breaches. Security measures have to be developed and built into every system when they are created and older legacy devices have to be updated or replaced to provide maximum security against threats. Security is a process not a product and this means that security settings have to be updated and constantly reviewed by including firewalls, encryption capabilities, authentication and control with proper security policies that support and enforce all the necessary security measures.

Protocols can be purchased and sometimes source code of a particular device can be found online, which therefore gives a potential attacker the opportunity to find faults in the code and study it in order to find a way to harm the system. Installing a device in a standalone manner, and not connecting it to the network can be one of the solutions to prevent unauthorized access,

but this prevents the utility benefitting from all the capabilities that the device has to offer. Using standards and common protocols means that systems are getting exposed, and attack surfaces are getting bigger. Establishing an extensive access control system and removing possible vulnerabilities that can be used by attackers to access substation automation systems is one way to improve security.

The purpose of an access control mechanism is to protect critical system resources by limiting access to only for the designated entities [8]. The most important task of substation security is to protect the equipment and its functionalities so they can deliver electrical power to the customers without interruptions [9]. Physical and cyber-security controls therefore should complement each other by becoming a layered defense providing confidence in the security of the whole system.

1.2 Role-Based Access Control

RBAC is a method for regulating access to a resource based on the relationship between the requester and the organization, meaning that the requester's role will determine if the access to perform a particular task will be granted or denied [8]. RBAC, therefore, states that no user should be given more rights than is necessary to do the job. For example, operators should be given control privileges and protection engineers will be given the authority to change settings in protection and control devices.

Table 1.2.1 List of pre-defined role-to-right mapping [8]

RIGHT / ROLE	VIEW	READ	DATASET	REPORTING	FILEREAD	FILEWRITE	FILEMNGT	CONTROL	CONFIG	SETTINGGROUP	SECURITY
VIEWER	X			X							
OPERATOR	X	X		X				X			
ENGINEER	X	X	X	X		X	X		X		
INSTALLER	X	X		X		X			X		

SECADM	X	X	X			X	X	X	X	X	X
SECAUD	X	X		X	X						
RBACMNT	X	X					X		X	X	

Table 1.2.1 reflects the minimum set of roles that have to be supported in a power system according to the IEC62351-8 standard. No role separately can get the full access to all the rights, but a responsible entity can assign several roles for one user. For example, a user can have roles like operator and engineer. When accessing the device as an engineer, the user can change configuration settings but in order to have the right to perform control commands, the user must log in to the IED as an operator. Every utility can also create additional roles with specific rights.

RBAC has the potential to reduce complexity in networks with a large number of IEDs [8]. In order to delete, add or modify roles and their rights, each device has to be configured separately. To do this in bulk, changing and modifying users in a hundred or more IEDs is very labor-intensive, time-consuming and often requires the utility to physically send someone to the substation. A possible solution is to use RBAC with centralized authentication system.

1.3 Decentralized and Centralized Authentication

For small networks, a decentralized authentication system is the simplest method to provide security against unauthorized access. The list of users can be stored in the IED, but this approach creates several vulnerabilities and difficulties when managing multiple devices:

- Each IED has to be manually updated when any changes are done.
- If an employee leaves the company then deleting the user account within a certain period can be difficult when there is no synchronization mechanism available between the IEDs in the network.
- It is difficult to have individual user accounts. When changes are made by the user, for example, when the user changes his/her password, then this has to be updated in each IED manually. [2]

Centralized authentication is able to remove these difficulties. With this type of authentication, the device connects to the authentication server to validate user credentials and when a change

occurs, for example, the user changes password, then that will be reflected in each connected device when the next validation occurs. The biggest advantage of centralized authentication is that the user list can be managed in a single location without going from one device to another. Changes made to the user list are available either immediately or the next time the device validates user credentials from the server. Therefore, centralized authentication of user accounts and roles provides a more efficient user management system compared to a decentralized solution. If a user leaves the company or gets promoted and will be assigned a new role, access to the substation equipment can be modified or revoked from a single centralized location. [2]

Centralized authentication is, therefore, the logical approach for creating a centralized user authentication system that can handle IEDs in the substation network, but this method also has its difficulties:

- An initial trust relationship has to be established between the centralized authentication server and the IED.
- A reliable connection between the centralized authentication server and the IED needs to be created and maintained when there is a need to verify credentials.
- Data sent over the network has to be protected.
- When the centralized authentication server is offline, local access to the IED has to be made possible. [2]

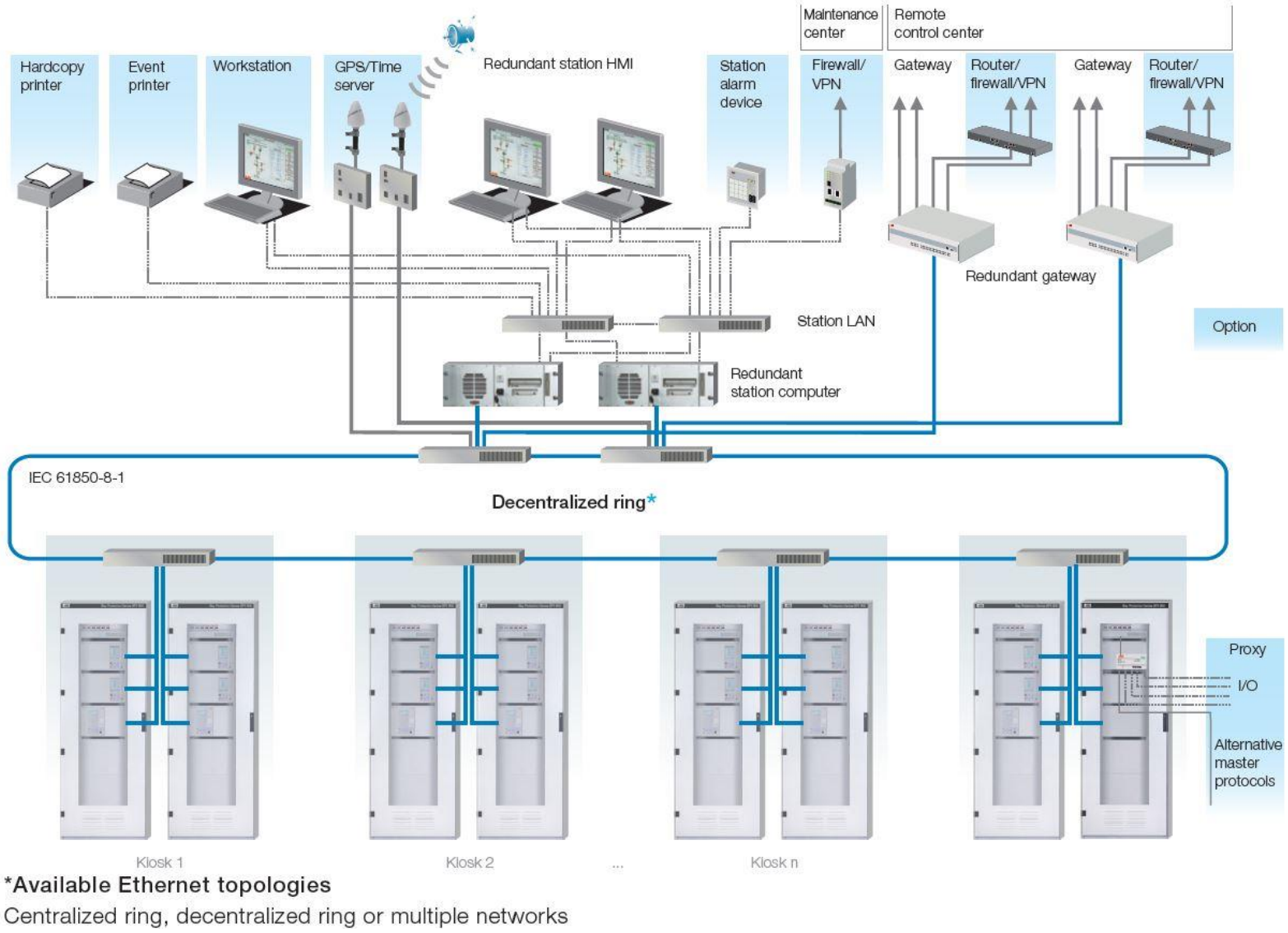

Figure 1.3.1 Substation network diagram [10]

Figure 1.3.1 shows a typical substation network that consists of multiple IEDs that are connected to the remote control center. It is difficult to manage users in each IED but by introducing a centralized authentication server, the modification can be made once in a single location and replicated to the IEDs. Not only does this save precious engineering hours, it also helps to follow standards and requirements.

According to the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection standard: *the responsible entity shall revoke such access to Critical Cyber Assets (CCA) within 24 hours for personnel terminated for cause and within seven days for personnel who no longer require such access to CCA* [11]. This means that the utility has to be able to revoke access to its IEDs for that particular person in 24 hours when an employee is terminated for cause in order to follow the NERC requirements. A midsized utility may have hundreds or even thousands of intelligent devices that have to be configured in 24 hours. Doing this manually, connecting to each device one by one and deleting the user account is a difficult task for anyone especially when there is no Virtual Private Network (VPN) connection established and the utility has to send an engineer to one substation after another.

In order to act in accordance with the requirements and to follow the standards, utilities have started to demand solutions from the manufacturers. As the market has now fuelled the demand, substation automation equipment vendors have to look into creating secure centralized authentication systems.

2 Secure Communication

2.1 Overview

To create trust in the substation automation network and to implement a centralized authentication system, it is important to use a mechanism that secures the information that is sent from one entity to the other. In order to send data over an unsecured network, the information has to be made unreadable.

A possible solution is to use cryptography, which is a process of using secret codes to secure the transmission of information over an unsecured network. That is done by using encryption that converts messages from readable plaintext into unreadable ciphertext. [1]

2.2 Encryption

There are two encryption methods currently available, these are symmetric key and asymmetric key encryption. The symmetric encryption uses the same key to encrypt and decrypt data, and the key is used to transform a message from plaintext into ciphertext in order to make it unreadable by parties who do not have the key. As long as both the sender and the receiver have the key, their messages can be sent in a secure way. [12]

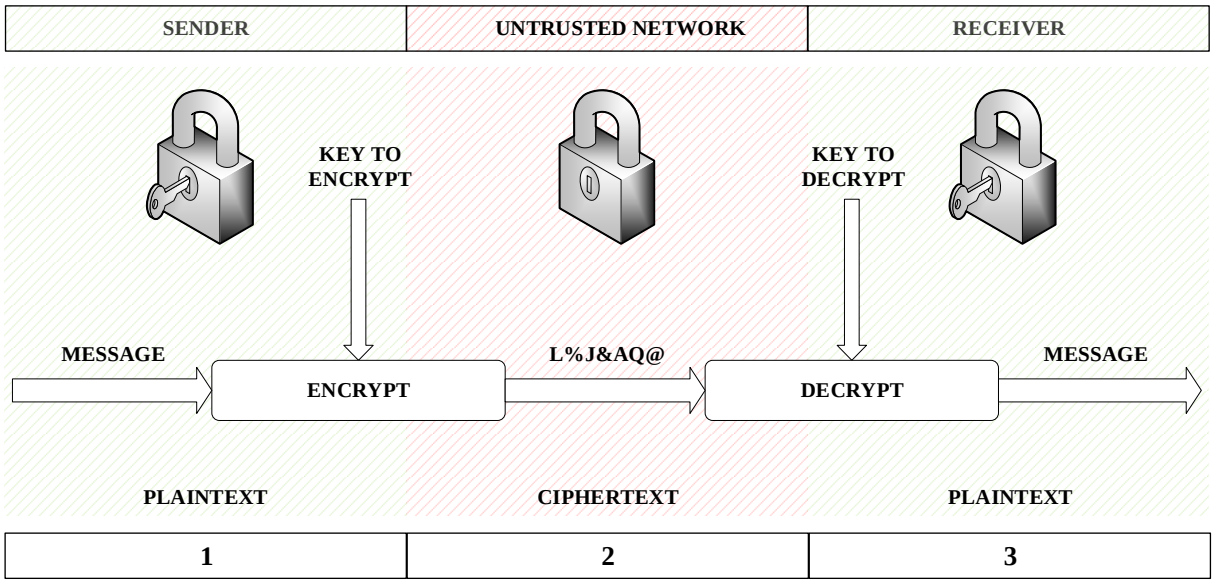

Figure 2.2.1 Symmetric encryption and decryption process

The symmetric encryption process on figure 2.2.1 is as follows:

1. The sender encrypts the plaintext message (MESSAGE) with a symmetric key.
2. Over an untrusted network, the message is sent as ciphertext (L%J&AQ@).

3. The receiver decrypts the message back to plaintext (MESSAGE) using the same symmetric key.

The problem with using symmetric encryption is that the key needs to be stored securely and in order to decrypt the message, the receiver has to have the same key that was used by the sender during the encryption process [12]. Although this option can be considered reasonable when both parties are in possession of the key, what if the device on the other end of the communication line does not have the symmetric key? This means that a secure channel would need to be created between the sender and the receiver in order to transfer the key. The problem is that it is difficult to send the key over an unsecured network without the untrusted third party possibly obtaining it. In order to exchange data in an environment where third parties may see the movement of information, it is important to use a more suitable method.

A possible solution is to use Public Key Infrastructure (PKI). The IEC62351-2 standard defines PKI as: *a system of CAs that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography* [13]. Therefore, PKI is a system that is used to attest that a public key belongs to an entity. Digital certificates are based on asymmetric cryptography, which uses a pair of keys for encryption and decryption [14]. The public key does not need to be a secret and the encryption can be done without the private key and therefore the private key does not need to be transferred.

The public key and the private key are created at the same time by the issuing CA and it uses a mathematical algorithm to create both the private key and the public key, and the keys cannot be derived from each other [15]. This means that if the public key ends up with a third party the message can't be decrypted without having the private key. Therefore, the public key can be distributed over the network, but the private key has to be kept secret by its owner otherwise if the private key is compromised, a third party can decrypt the message and the confidentiality is lost.

When information is encrypted with the receiver's public key, it is done in a way that there are a large number of possible solutions available, therefore creating a puzzle with endless outcomes. In order to decrypt the data, the attacker has to test every single solution in order to obtain the information. The secret private key adds enough information to the puzzle to enable the receiver to decrypt the message. As mentioned previously, the process is possible because the public key and the private key are both mathematically connected to each other [16].

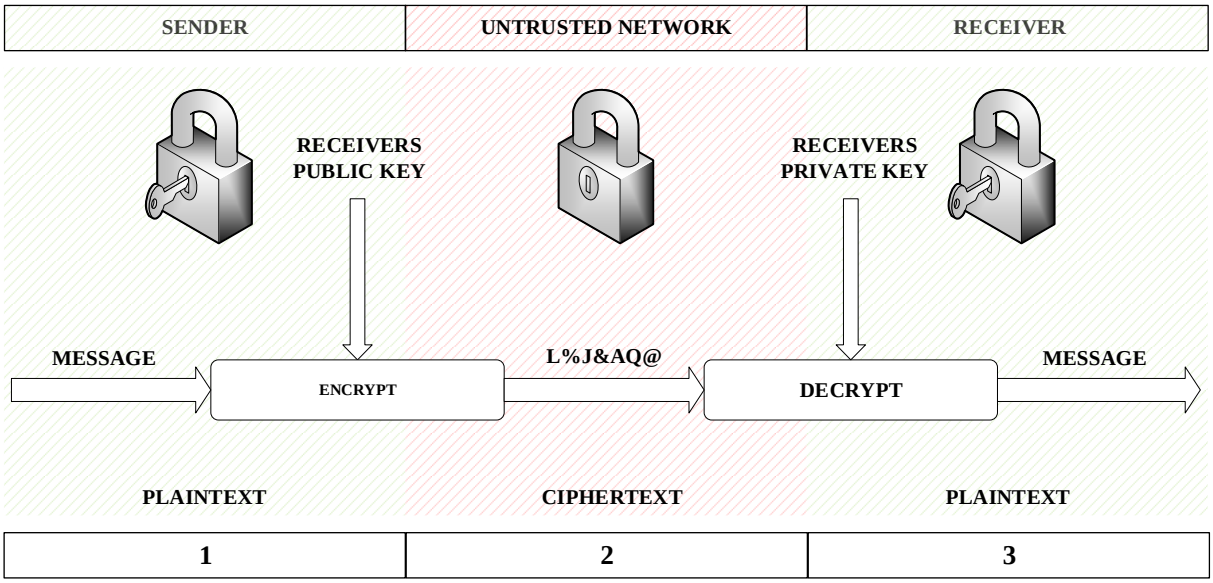

Figure 2.2.2 Asymmetric encryption and decryption process

The asymmetric encryption and decryption process on figure 2.2.2 is as follows:

1. The sender encrypts the plaintext message (MESSAGE) with the receiver's public key.
2. Over an unsecured network, the message is sent as ciphertext (L%J&AQ@).
3. The receiver decrypts the message back to plaintext (MESSAGE) using its private key.

The asymmetric encryption and decryption process therefore uses different keys and every entity in the network has their own private key and a public key. The message is encrypted with the receiver's public key and can only be decrypted with the receiver's private key therefore making the communication between two entities secure when the parties are in possession of their secret private key. Asymmetric encryption, therefore, can play an essential role in securing communication between the centralized authentication server and the IED.

2.3 Digital Certificates

In order to implement a centralized authentication system, it is important to know precisely who is requesting access information from the server. Therefore, the authentication server has to be able to verify that:

- The device sending the request is the originator and a trusted entity.
- The received data integrity has not been compromised.
- The device receiving the information is the intended recipient.

The client connecting to the authentication server has to be able to verify that:

- The server is a trusted entity.

- The received data integrity has not been compromised.

This means that in order to address security in the substation network it is important that the connecting entities provide proof of trustworthiness. This can be done by exchanging digital certificates that are authenticated by a trusted third party. The digital certificate is used to bind the certificate holder's identity with its public key [3]. Therefore, a digital certificate is essentially an electronic file with data in it that is used to prove ownership of a public key that is sent along with the certificate. They are used to identify devices over communication networks and can enable secure and confidential communication between two parties using encryption. A certificate contains identification information about its owner and about the CA that issued it, for example [17]:

- Owner of the certificate- to which device the certificate was issued to.
- Validity period of the certificate- used to check that the certificate is not expired.
- A serial number- used to verify that the certificate has not been revoked.
- The certificate holder's public key- used to encrypt the response to the certificate owner.
- The name of the CA that issued and signed the certificate- if the CA is known and trusted by the receiver then the certificate can be considered trustworthy.

Therefore, in order to provide trust, the certificate should be issued and signed by a trusted third party, the CA, and the CAs signature verifies that the information in the certificate is not altered. If the certificate is modified by an unauthorized individual then the digital signature will not match the data in the certificate and the receiver of the certificate should not accept it [17].

2.4 Third Party Trust

Every security system depends on trust among its users. In order to trust a connecting entity, it needs to be certified as trustworthy by a third party. To be trusted in a network, two individual systems can enter into mutual trust through a common third party that vouches for the trustworthiness of the two connecting entities. [16]

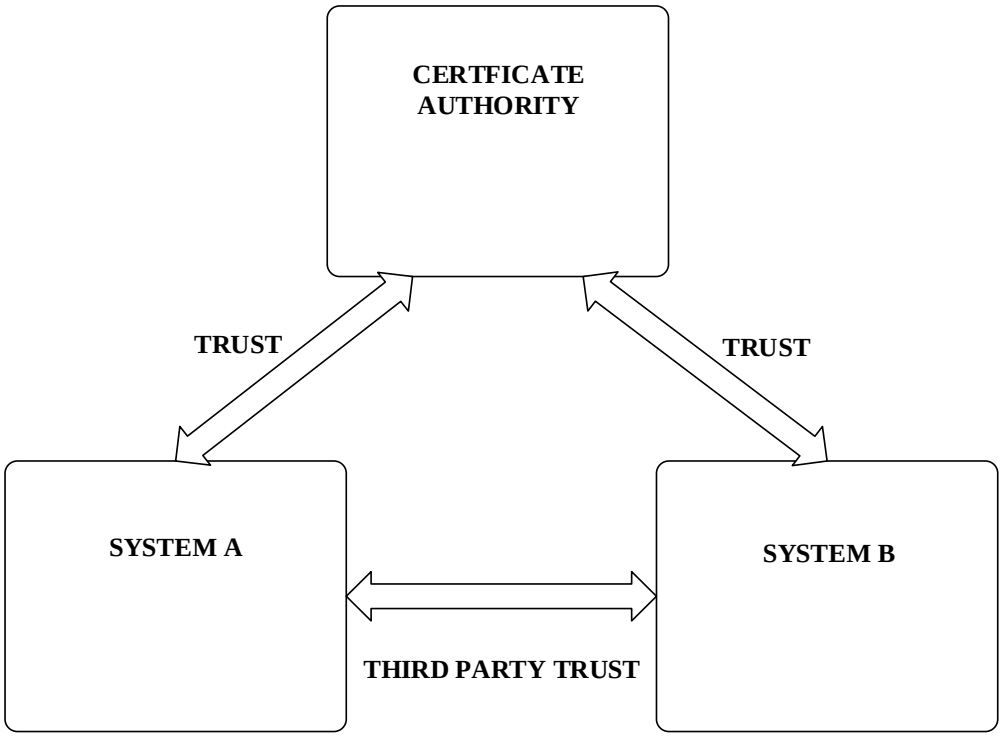

Figure 2.4.1 Third party trust model

Third party trust can be provided by a CA. The CA is a trusted entity that vouches for the trustworthiness of the two connecting systems and its responsibility is to create and sign certificates, and connect them to an asymmetric key pair, the private and public key. When the CA signs a certificate, the certificate holder can present it to the recipient to give proof of its identity. The CAs signature, is the proof that this particular system is trusted by a third party, therefore trusted by the CA. [17]

If the CA has issued and signed a certificate for an IED, the IED can communicate with an external server and provide proof of trustworthiness and ownership of the public key by presenting the certificate that is trusted by the third party, the CA. This method enables the server to verify that the connecting client is trusted. The certificate, issued and signed by the CA, is the IEDs electronic identity. This means that through third party trust, any device trusting the CA should now trust the IED.

The CAs signature provides proof that the certificate is valid and therefore legitimate. The entity verifying the certificates signature can be certain that only that particular CA has signed as it has access to its private signing key. [16]

For a CA to be trusted, it must be verified by a higher CA. There can be many different levels of CAs that all rely on the highest level, on the Root Certificate Authority (R-CA) [12]. The CAs down the trust chain automatically inherit the trustworthiness of the R-CA, and they can

provide proof of their trustworthiness by presenting their certificates with the R-CAs signature. There can be multiple Subordinate Certificate Authorities (S-CAs) and Intermediate Certificate Authorities (I-CAs) but there can be only one R-CA for a particular chain [12]. The R-CA should be removed from the network after the creation of the I-CAs and the S-CAs. This is important because the R-CA is the trust anchor and the whole certificate infrastructure relies on its signing private key, therefore losing its private key may compromise the whole system. The I-CA and the S-CA can still issue and sign certificates, therefore the system will work without the R-CA being online.

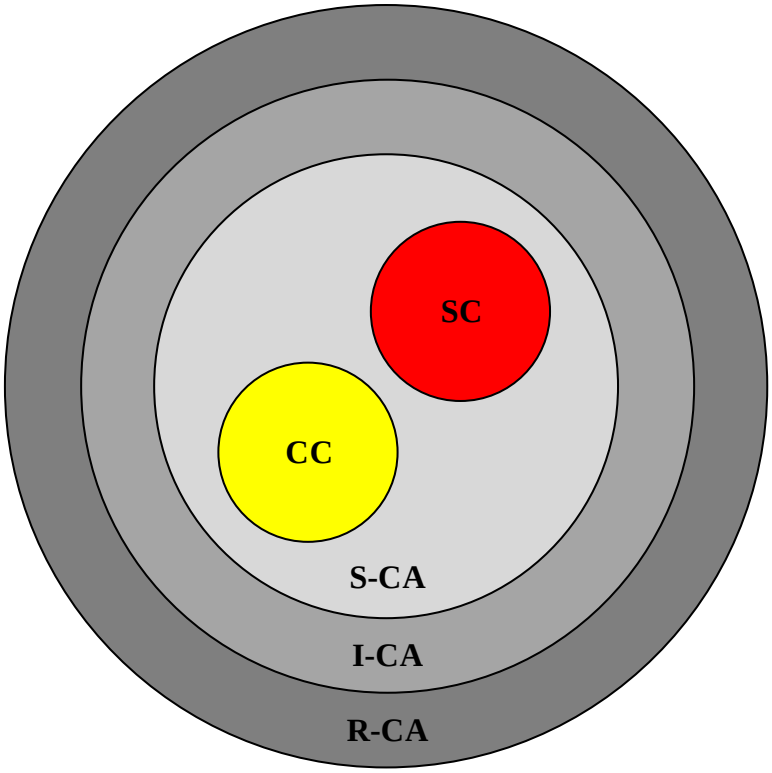

Figure 2.4.2 Layers of Certificate Authorities

The figure 2.4.2 shows layers of CAs that all rely on the R-CA. Client Certificate (CC) or SC is signed by the S-CA that signed by the I-CA and the I-CA is signed by the R-CA. CAs further down the trust chain inherit the trustworthiness of the R-CA. There can be many S-CAs and I-CAs but there can only be one R-CA. The previous diagram can also be outlined as following:

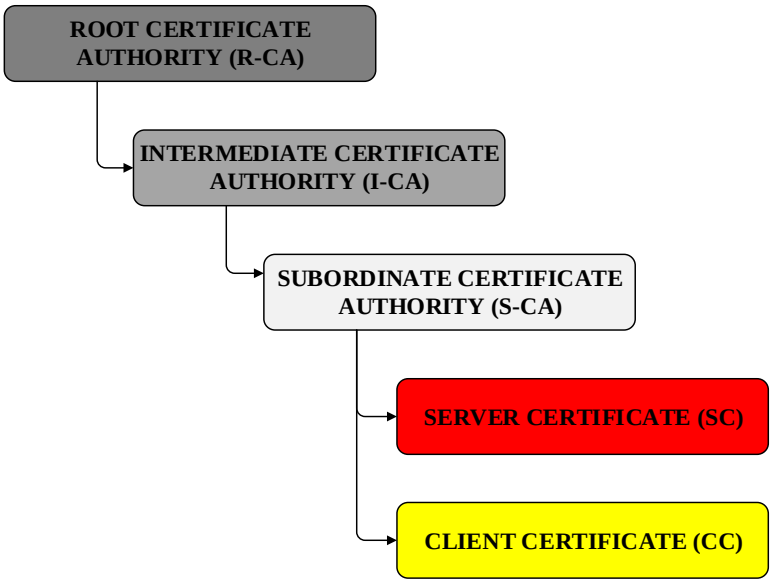

Figure 2.4.3 Certification path

According to figure 2.4.3 the R-CA signs the I-CA that signs the S-CA. The final CA, the S-CA, signs the CC and the SC. As seen on the figure, a trust chain is created and when a certificate receiver wants to verify the certificates integrity it has to verify the signing CA and if the CA is not known then the receiver needs to verify an upper-level CA. If the CA is known then the certificate can be trusted. If the certification path can't be verified then the certificate should not be accepted.

The R-CA is usually self-signed by its own private key [12]. The CAs further down the trust chain all rely on the R-CA and therefore its security is vital for the rest of the system. If the R-CA is compromised then the CAs and certificates relying on it have to be revoked and cannot be accepted by the receiving entities. The CC and the SC can be signed by different CAs but the receiver has to have the possibility to verify the signing CA by verifying its signature and by checking its list of trusted CAs that, therefore should be stored inside the device that verifies the certificate.

2.5 Transport Layer Security

This is where symmetric/asymmetric encryption and certificate exchange all come together. *The TLS protocol uses digital certificates to create a secure, confidential communications channel between two entities* [17]. Therefore, TLS is a security protocol that can provide the necessary privacy for sending authentication information over to the centralized authentication server. TLS is used to encrypt the connection between two entities over an unsecured network

and it can be used to create a secure connection between the IED and the centralized authentication server.

As mentioned before, the motivation to use certificates is to provide trust in the network. Presenting a valid certificate that is trusted by a third party, the CA, provides assurance that the connected device is legitimate. TLS combines symmetric and asymmetric encryption, therefore providing a way to secure the connection between two entities [17]. As mentioned previously in chapter 2.2, symmetric encryption works only when both entities are in possession of the key, but sending the key over an unsecured network is dangerous, so symmetric encryption alone should not be used. In order to provide a way to send symmetric encryption keys over the network safely, it is important to encrypt the symmetric encryption keys. This is where asymmetric encryption comes in, the symmetric key can be encrypted with the receiver's asymmetric public key, therefore providing security when sending the key over the network. The receiver can decrypt the symmetric key with its asymmetric private key. After the decryption, both parties have the symmetric key that can be used to send messages securely over the network. Therefore, asymmetric key encryption is used to exchange keys and symmetric key encryption is used to encrypt the transferred data.

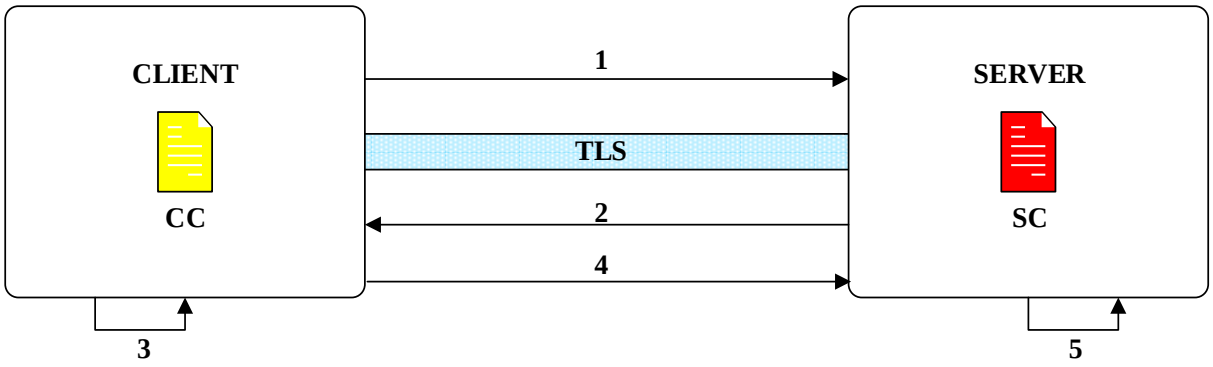

Figure 2.5.1 TLS protected session between the client and the server

The TLS session encryption process on figure 2.5.1 is performed as follows:

1. The client sends a request to the server to establish a TLS protected connection.
2. Server responds by sending its SC and its asymmetric public key.
3. The client checks the SC and verifies the CA that issued it.
4. The client generates a unique symmetric key and encrypts it with the server's asymmetric public key. The client then sends it to the server and if requested the client will add its CC.
5. The server verifies the CC and decrypts the symmetric key with its own private key.

The TLS protected connection is now established and both the client and the server, who both have the only two copies of the same symmetric key, can use it to send encrypted messages to each other. TLS, therefore should be used to establish a secure connection between the IED and the authentication server and to identify the connecting entities.

3 Centralized User Account Management Process

3.1 General

As discussed in chapter 1.3, a centralized user account management system ideally should be quick to verify credentials without exposing any user information while the data is in transit or stored and it needs to provide reliable answers. Therefore the goal for a centralized user account management system in a substation environment is to ensure that only authorized personnel are allowed to access the necessary devices, to prevent errors made by the designated users, and to protect the substation network from unauthorized access. This is difficult to achieve as during the authentication process, the password will be sent to the server for verification but what happens if the server turns out to be compromised? Similarly, as the server contains valuable user information, it needs to be protected from a compromised client and from direct attacks. Critical information needs to be protected from unwanted exposure and security controls have to be established.

3.2 Overview of Lightweight Directory Access Protocol

A suitable method to exchange user information between the authentication server and the IED, is to use LDAP. LDAP is an access protocol for directories, and it offers a way to search, collect and change information over a network and it enables the system administrator to manage and store authentication information in a centralized location. In LDAP, authentication is done with binding a user to a particular entry in the directory. Its directory is organized in a hierarchical manner and the data can be replicated between different servers, which are then synchronized periodically. The directories contain information about the username, password, and the user's role. Rather than managing a list of users in each device, information in an LDAP server is stored in a single location and can be updated instantly so the connected devices can access the latest user information. [4]

LDAP supports different types of authentication. The simplest form of client authentication is to bind to the server's directory entry using a plaintext password but for security reasons, this method should not be used [18]. Network scanners are able to pick up data and replay it later to gain access to the system. To prevent any unauthorized access and modifications, certain security and authentication options have to be enabled. Because LDAP supports TLS, data confidentiality and integrity can be protected while it is in transit and certificates should be used to prove a client's identity to the server and the server's identity to the client [4]. With this

approach, the risk of exposing passwords can be taken to minimum. The negative aspect of this approach is that the system gets more complicated and requires creating certificates for IED in the network. But in order to gain security, this approach should be implemented.

As mentioned in chapter 1.2, RBAC is a technology that can simplify security administration through the use of roles and constraints to organize access for users. In order to implement a centralized authentication system with RBAC and LDAP, the standard IEC62351-8 defines two general models. The first option is to use the PUSH model where the subject can fetch the access token from the repository of the identity provider, in this case the LDAP server, to access the object. [8]

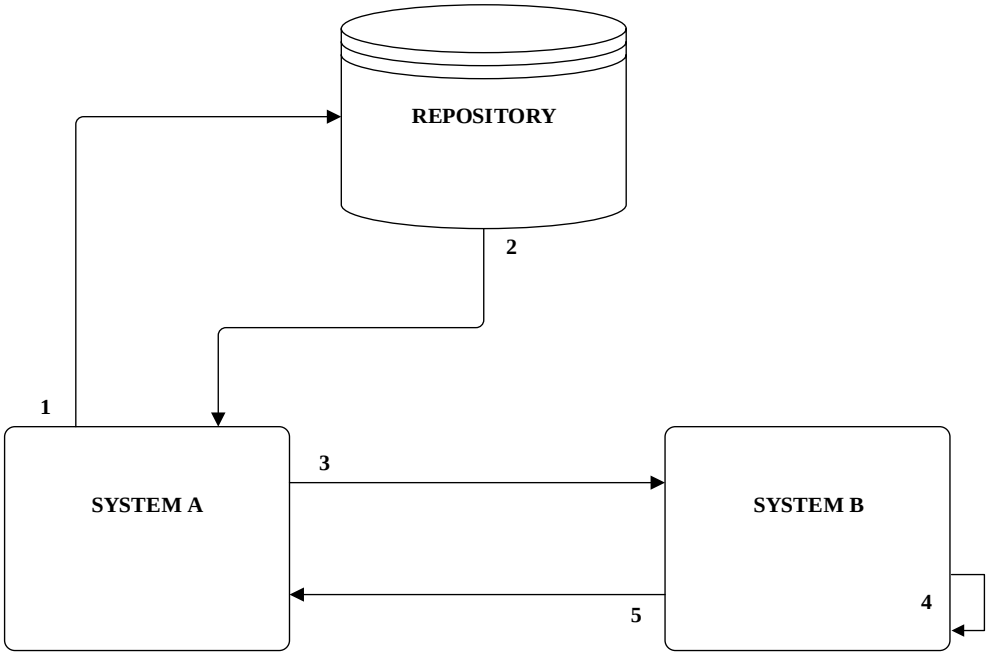

Figure 3.2.1 LDAP PUSH model based on RBAC

The PUSH model authentication process on figure 3.2.1 is performed as follows [8]:

1. The user on system A, authenticates itself to the repository in order to get the access token containing the roles.
2. The repository provides system A with a token that contains the roles.
3. System A provides system B the token that contains the roles.
4. System B verifies the token and gives access to the user according to the roles.
5. Acknowledgment from system B to system A.

To support cases, where the device do not have the appropriate interface, for example an IED with simple Human-Machine Interface (HMI) with a display and a key pad to provide the access token locally, a more suitable method is needed. According to the IEC 62351-8 standard, the

second option is to use the PULL model where the access token can be fetched by the object from the repository of the identity provider, in this case the LDAP server, when the subject connects to the object. [8]

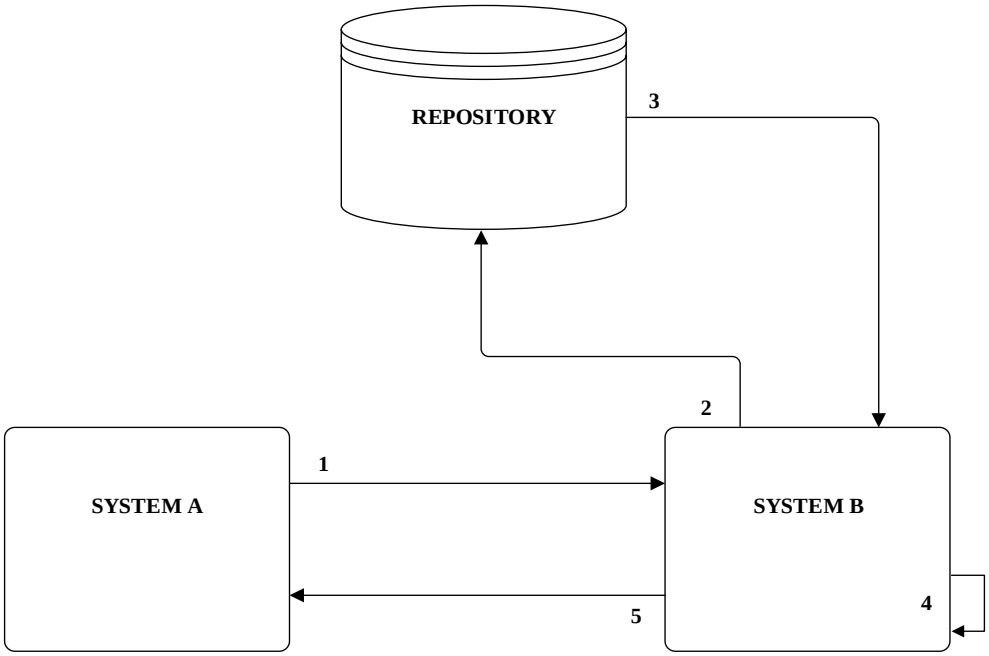

Figure 3.2.2 LDAP PULL model based on RBAC

The PULL model authentication process on figure 3.2.2 is performed as follows [8]:

1. System A opens a TLS protected channel to system B. After verifying the identity of system B, system A sends the user credentials to system B.
2. System B verifies the user credentials from the repository. TLS protected channel should be used to protect the transferred information and to verify each connecting entity.
3. System B retrieves the token containing the user roles.
4. System B verifies the access token.
5. System B either permits or rejects access towards system A.

Often in substation automation systems users need to accesses the IEDs using their local HMI without having a separate platform to enter credentials. If this is the case, system A and system B would coexist as one. Comparing the PUSH and PULL model, it is clear that PUSH model is not suitable for a system with IEDs that have simple HMIs in terms of a key pad and a display. In order to accommodate a particular IED specifics, PULL model should be used.

3.3 User Authentication Process

Using the PULL model, which is described in chapter 3.2 as an example, the user authentication through an LDAP server can be done as explained on the figure 3.3.1. This can be also called IED in online mode.

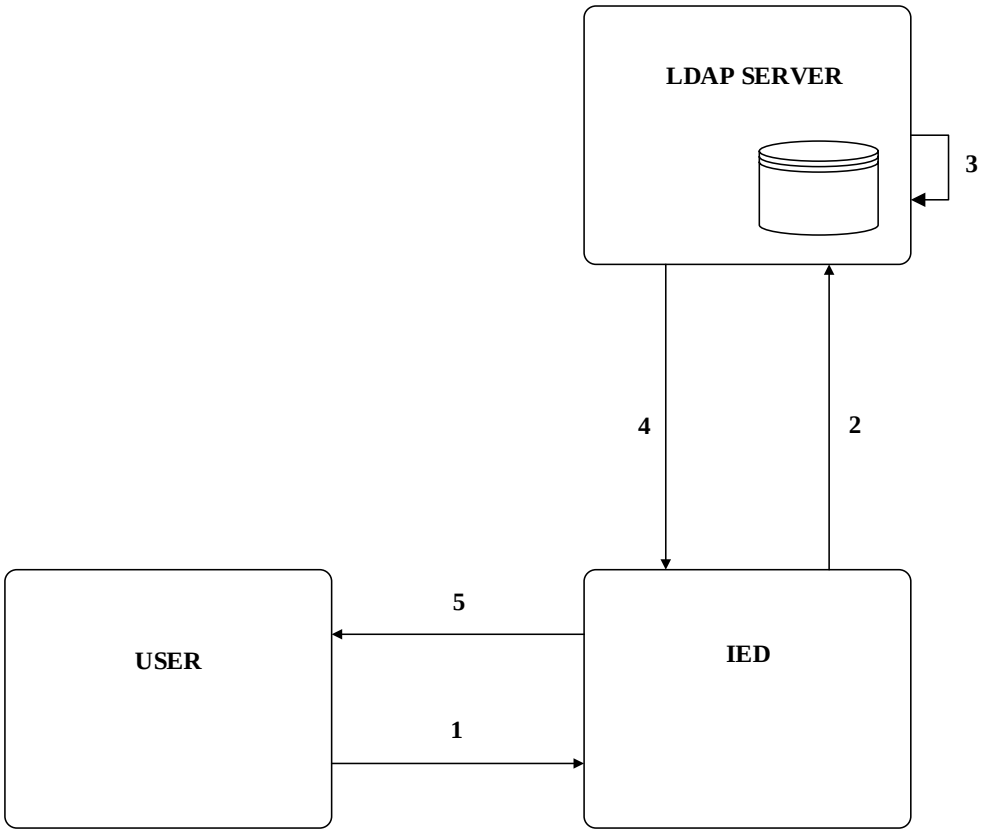

Figure 3.3.1 User authentication in online mode

The authentication process, based on PULL model, on figure 3.3.1 is performed as follows:

1. User sends credentials (name and password) to the IED.
2. The IED sends a bind request to the LDAP server to authenticate the user.
3. The LDAP server searches its directory for an entry that matches the username. After checking the username, the LDAP server compares the user password with the one that is found in the LDAP server. If they match then proceed to step four, if not then access is declined for the user.
4. LDAP server binds the user to a role and sends a token containing the roles to the IED.
5. User picks the role and accesses the IED.

It must be noted that in step three, if the user name or password does not match with the one in the LDAP directory then the user should be prompted with an error message and access is denied. LDAP server also checks the validity of the user's password and if it has expired the

user should be prompted to change it before accessing the IED. The password can be changed either using the HMI, the vendor specific IED configuration tool or by connecting directly to the LDAP server.

3.4 Security Concerns

Authentication is an important security mechanism. It is necessary that only authorized control actions are allowed to take place in a substation and therefore it is crucial to allow access only for the designated entities. This creates a need to protect the system and the information flowing between the devices. Adding a centralized user authentication system introduces several vulnerabilities into the substation communication network.

When taking user information away from the IED and storing it in a server, that creates a possibility for an SPOF. A SPOF is essentially a situation when due to a breakdown, a device, in this case the LDAP server that is a critical part of a system, if it fails then the whole system stops working [3]. This would mean that users can't access IEDs anymore. An attacker or a malfunctioning device can also overload the network by creating an abnormal amount of data traffic creating a DoS, therefore making the system unusable for its designated users [13]. As availability is crucial in a substation, it is critical that an engineer can access the IED when needed. This means that redundancy is needed, and an offline authentication solution has to be developed in case the centralized authentication server, the LDAP server, is offline or malfunctioning.

An attacker can also spoof the connecting entity, either the IED or the LDAP server, to release sensitive information. This can be done by hijacking the IP address of the IED or the server and send invalid data to an unsuspecting entity by pretending to be a valid device. In a distributed client-server environment, a user needs to access a device using login credentials, which are sent over an unsecured network to the authentication server. While the information is in transit, it can be read by others who can use the information to cause harm. Therefore, there is a need to secure data while it is in transit. Not only is it important to protect data during transfer, it is crucial to authenticate entities in the network and request proof that they are trustworthy.

3.5 Single Point of Failure

A single centralized user authentication server is a potential risk for an SPOF, and the system can have a dangerous situation when an LDAP server is not accessible. Users will not be allowed to log in to the devices, and the whole system becomes inaccessible.

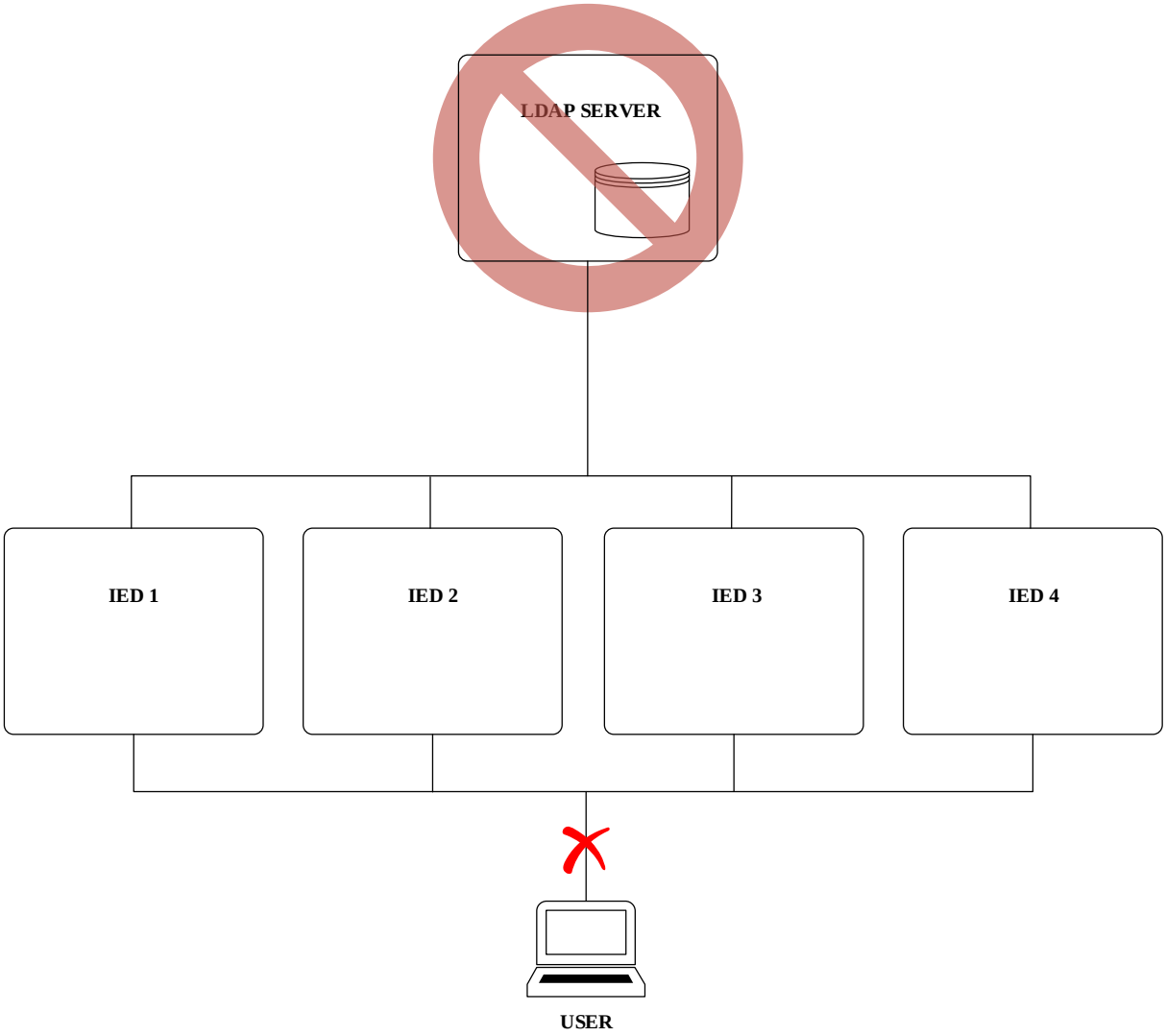

Figure 3.5.1 Logical drawing of a single LDAP server setup

Figure 3.5.1 shows multiple intelligent devices that are connected to a single LDAP server. If the only server fails then the devices will not be accessible and there is no possibility to authenticate credentials. All users will be locked out of the devices.

Maintaining access to substation devices is critically important as it is considered unacceptable if an authorized user cannot access the device. The information in the LDAP server can be frequently replicated to the backup servers in order to have the latest updates. Having multiple servers with replicated user information allows the system to work even if one of the servers fails. [4]

Therefore, for added reliability and security, substation IEDs can communicate with several LDAP servers to switch over to the backup one in case of a failure. The best way to reduce the risk of losing a centralized user authentication service and to add redundancy to the system is

to have a secondary and tertiary server available if the first one fails. If the first LDAP server cannot be reached, the IED tries to connect to the secondary LDAP server.

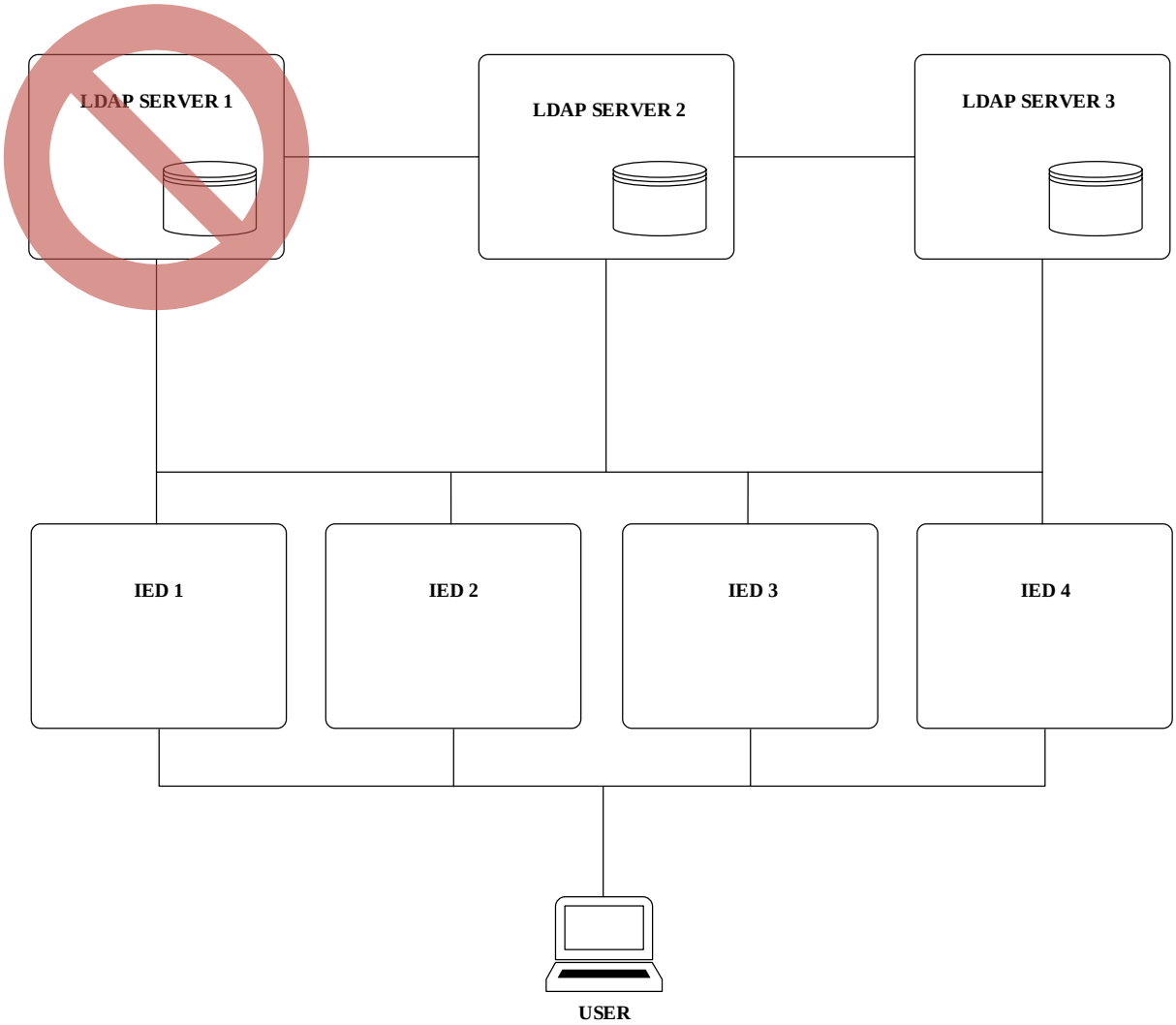

Figure 3.5.2 Logical drawing of multiple LDAP server setup

Figure 3.5.2 shows that the primary LDAP server (LDAP SERVER 1) has malfunctioned and the secondary LDAP server (LDAP SERVER 2) takes over the authentication from the primary LDAP server (LDAP SERVER 1). When the primary LDAP server (LDAP SERVER 1) is malfunctioning then the secondary LDAP server (LDAP SERVER 2) becomes the primary and the tertiary LDAP server (LDAP SERVER 3) becomes the backup, secondary server.

In the case of Wide Area Network (WAN) communications loss, the IED should also have a local repository inside the device. The repository should be an exact copy of a domain specific subset of the LDAP server's directory, and it should contain the username, the hash of the password and the user roles. It is important that the passwords should be stored in hash not in plaintext or in an encrypted form for added security. The data can be therefore written to the

IED repository when it is connected to the LDAP server, and it should be regularly updated. If the IED is offline, then it will use the locally stored credentials to authenticate the user. If the password has passed its validity date, then the IED should still allow the user to access the device because it is more important that the engineer has the possibility to access the IED than blocking access. If a user, who is not on the list, but wants to access the IED then access for that particular person is denied.

The following will explain the user authentication process when a user accesses an IED while it is in offline mode- not connected to the LDAP server.

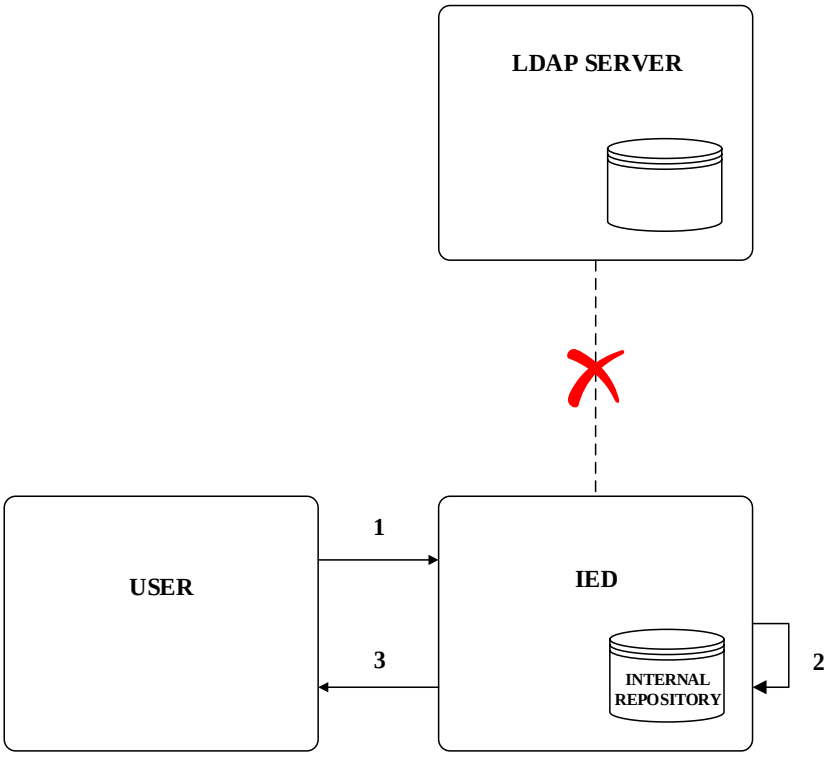

Figure 3.5.3 IED in offline mode

The authentication process in IED in offline mode, on figure 3.5.3, is performed as follows:

1. User types the username and password using the local HMI on the IED or the vendor specific IED configuration tool.
2. The IED checks the user input and compares it with the user name and the password from its local repository. If everything is valid then the user is given a role. If the input is invalid, then access is denied, and the user has to try again with the correct credentials.
3. User picks the role and accesses the IED.

In offline mode the password should not have an expiration date but the user should be prompted for a new password when the IED is connected again with the LDAP server.

The most preferred option is to implement both the backup LDAP servers for extra redundancy and the IEDs internal repositories in case the WAN communication is lost.

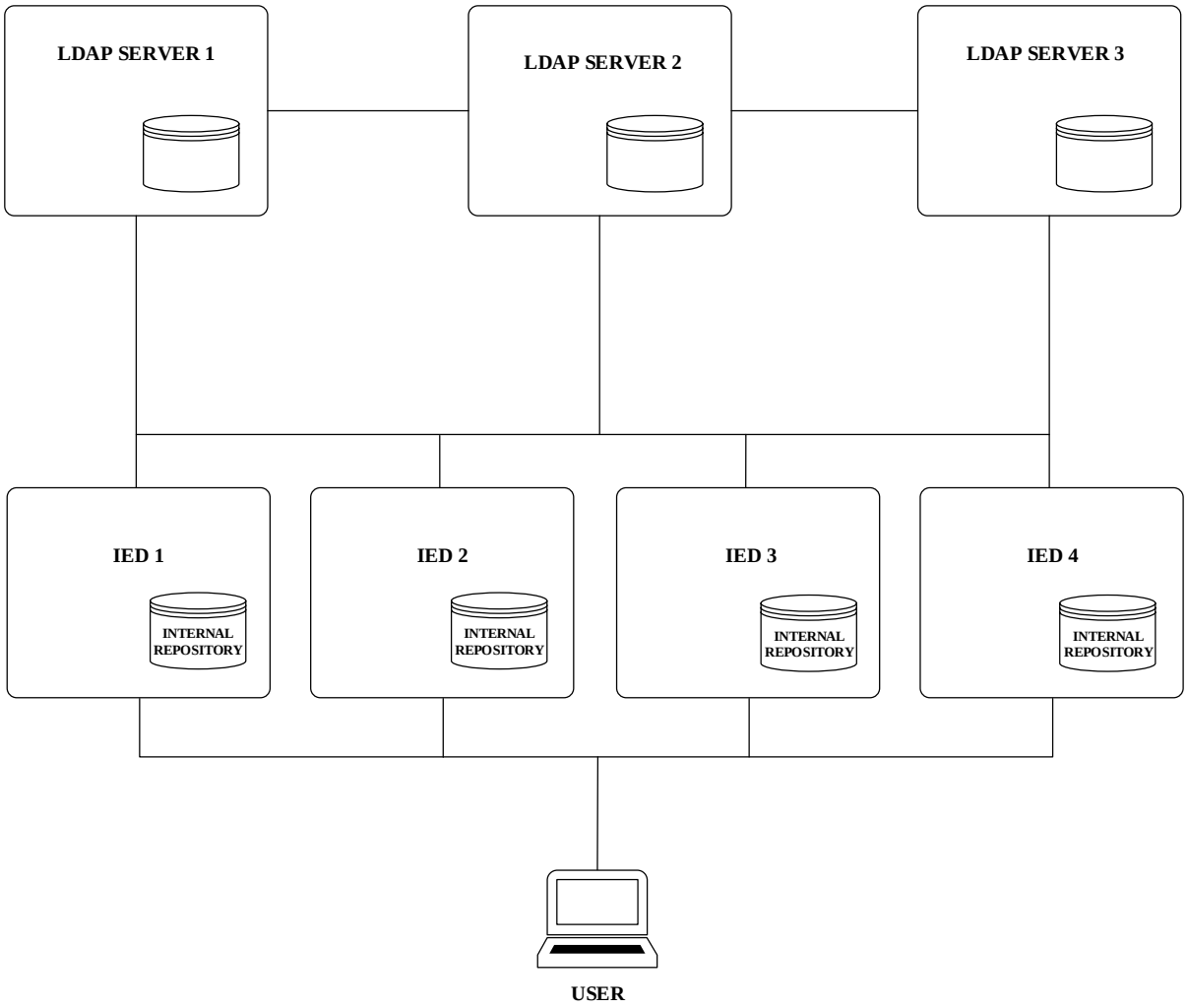

Figure 3.5.4 Combined solution with backup LDAP servers and IEDs internal repositories

Figure 3.5.4 shows the substation automation system with multiple LDAP servers, one primary and two for backup, and in case of WAN communication loss, the IEDs will have their own user lists in their internal repositories.

3.6 Denial of Service

A rogue or misbehaving client may overload the LDAP server and create a DoS by creating an abnormal amount of network traffic. This can make the user log in process extremely slow and prevent or even impede the whole system operation for the rest of the devices.

A rogue user can create and execute a script that creates log in requests to an IED, targeting the LDAP server with verification requests eventually saturating it so it cannot respond or it responds so slowly that the system becomes unavailable for its intended users.

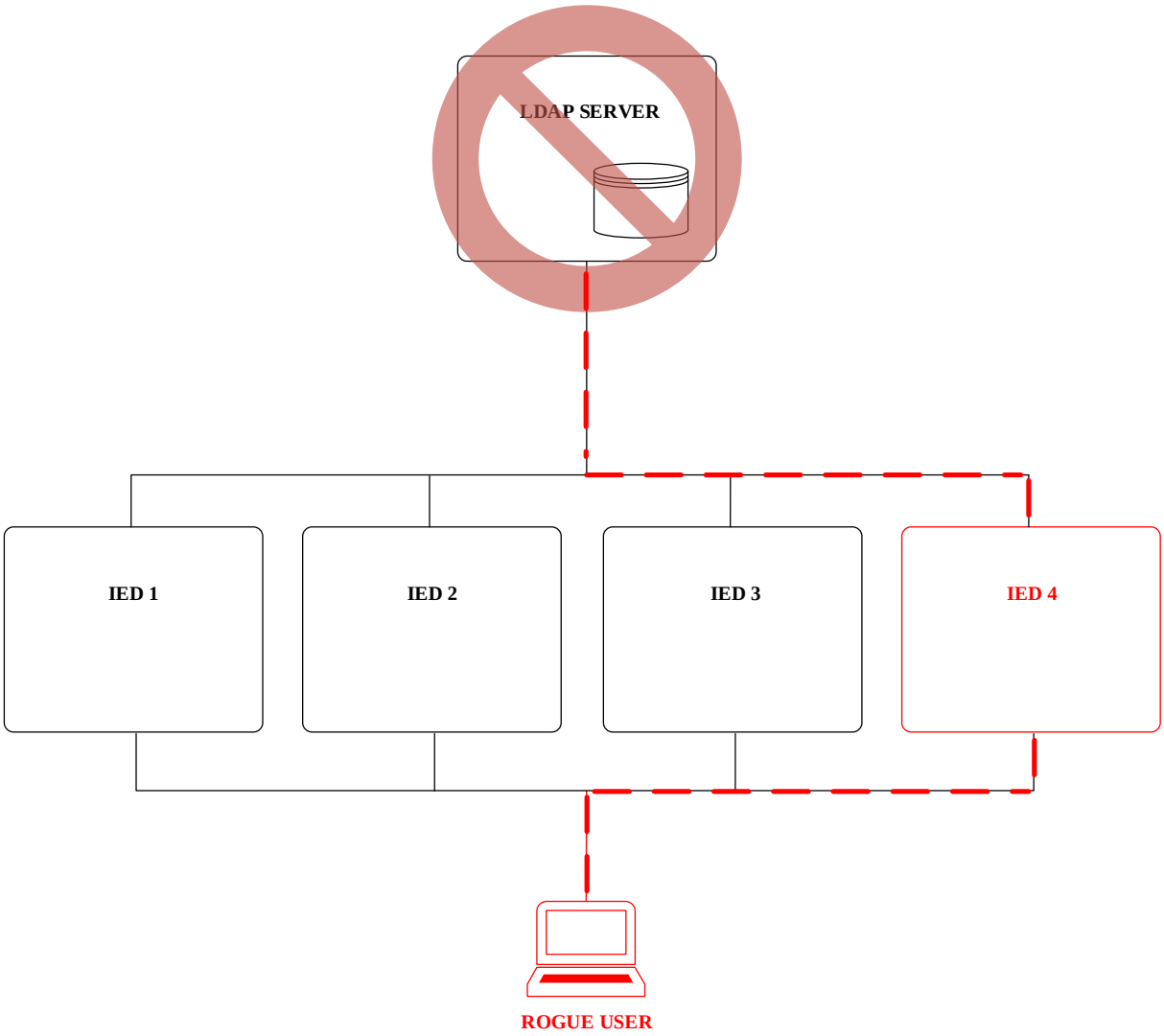

Figure 3.6.1 A rogue user in a substation communication network

Figure 3.6.1 shows a rogue user creating extensive amount of traffic in the substation network by overloading the LDAP server with queries and making the system unusable for the rest of the devices.

Precautions have to be set to avoid a situation where a user or a device accidentally or on purpose creates too much traffic between the IED and the LDAP server. In order to prevent a lockout from the device, it is important to use backup data that is retrieved from the LDAP server. When a user logs in to the IED, the IED will verify the credentials via the LDAP server and after receiving the roles, the user data can be stored within a cache for a specific time. When

the user logs out and in again between a certain timeframe and with the same credentials, no LDAP verification is performed, and the account information is verified from the cache. Only after a certain time the cached account will be deleted, and a new LDAP request has to be performed in order for the user to log in again. In case of multiple failed log in attempts the user will be blocked in most systems.

A rogue client can circumvent this by using a new username for each request and still create a DoS. If this is the case, the node should be banned in order to protect the whole network but it should be banned only for a specific time and the local access can be provided using the local repository. The IED can maintain a cache of credentials, the validity of this information must be limited in time to prevent unauthorized access by a user whose access rights have been revoked.

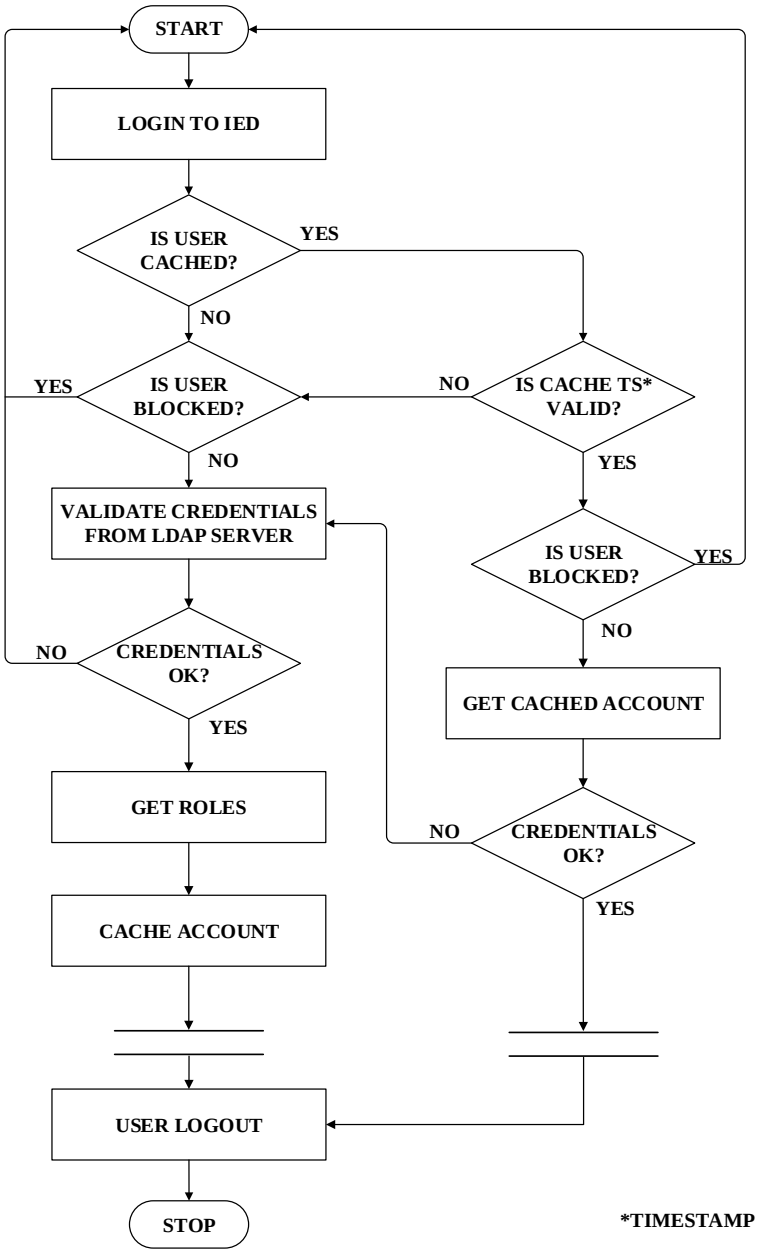

Figure 3.6.2 Logic diagram for caching a user account

Figure 3.6.2 is a proposed logic diagram for caching a user account. The process is as following, the user provides credentials to the IED, the IED checks its internal repository if the user's credentials are cached, if so then it will check the timestamp. If the timestamp is valid and if the user is not blocked then the IED checks the credentials. If they match then the user is allowed to access the IED. If the credentials are not stored in the repository or they are not updated or valid, then the IED sends a request to the LDAP server to verify the credentials, if the credentials match then the server sends the roles associated with the user. Afterward, the information is cached, and a timestamp is added as the IED cannot rely on the information forever. If the user is blocked then access is denied until the block has been removed after a certain time period.

LDAP servers can be configured to replicate data from and to a master server, so the read-only query load can be spread across as many machines as necessary [18]. This means that when a user changes a password that results in a change in the LDAP server's directory, then this will be referred back to the master server. Having a hierarchy of LDAP servers protects the most vital primary server and the query load is spread accordingly between the lower level servers.

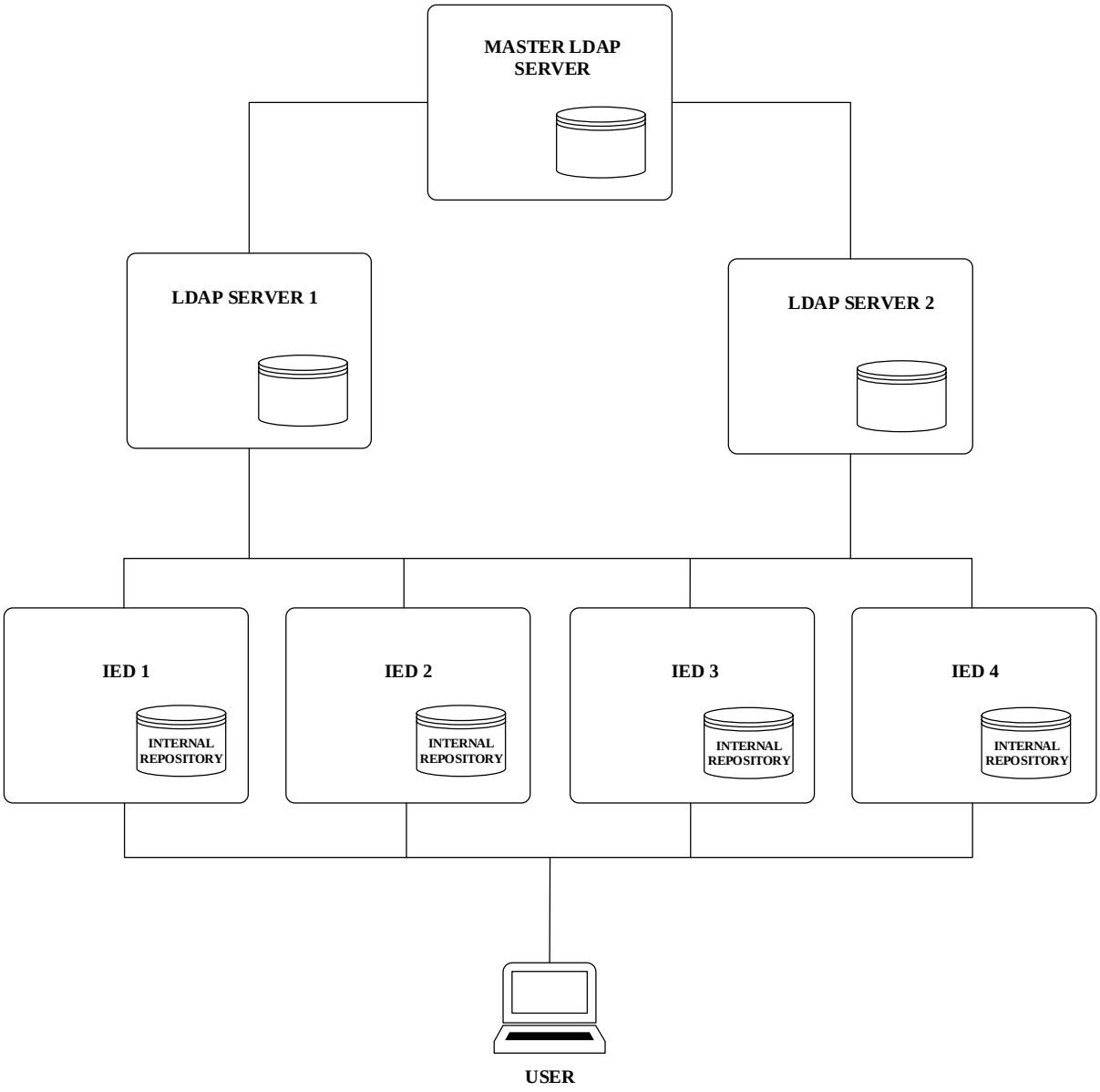

Figure 3.6.3 Master LDAP server

According to the figure 3.6.3, information to and from the LDAP SERVER 1 and 2 is replicated to the MASTER LDAP SERVER. An alternate means of authentication should also be provided to ensure local access in the event of WAN loss and therefore the IEDs should be equipped with a local user list.

3.7 Fake Server

If an intruder manages to gain access to a communication line without proper validation and authentication, they can execute control as if they were the privileged user. Anyone who would like to mimic a data source could have access to hundreds of machines at once, and they can possibly modify data in the client devices. Therefore, a fake LDAP server can be one of the most dangerous problems in a substation. Without a proper client-server validation, a fake LDAP server can grant a rogue user all possible access rights, including redirecting later LDAP requests to an illegal LDAP server.

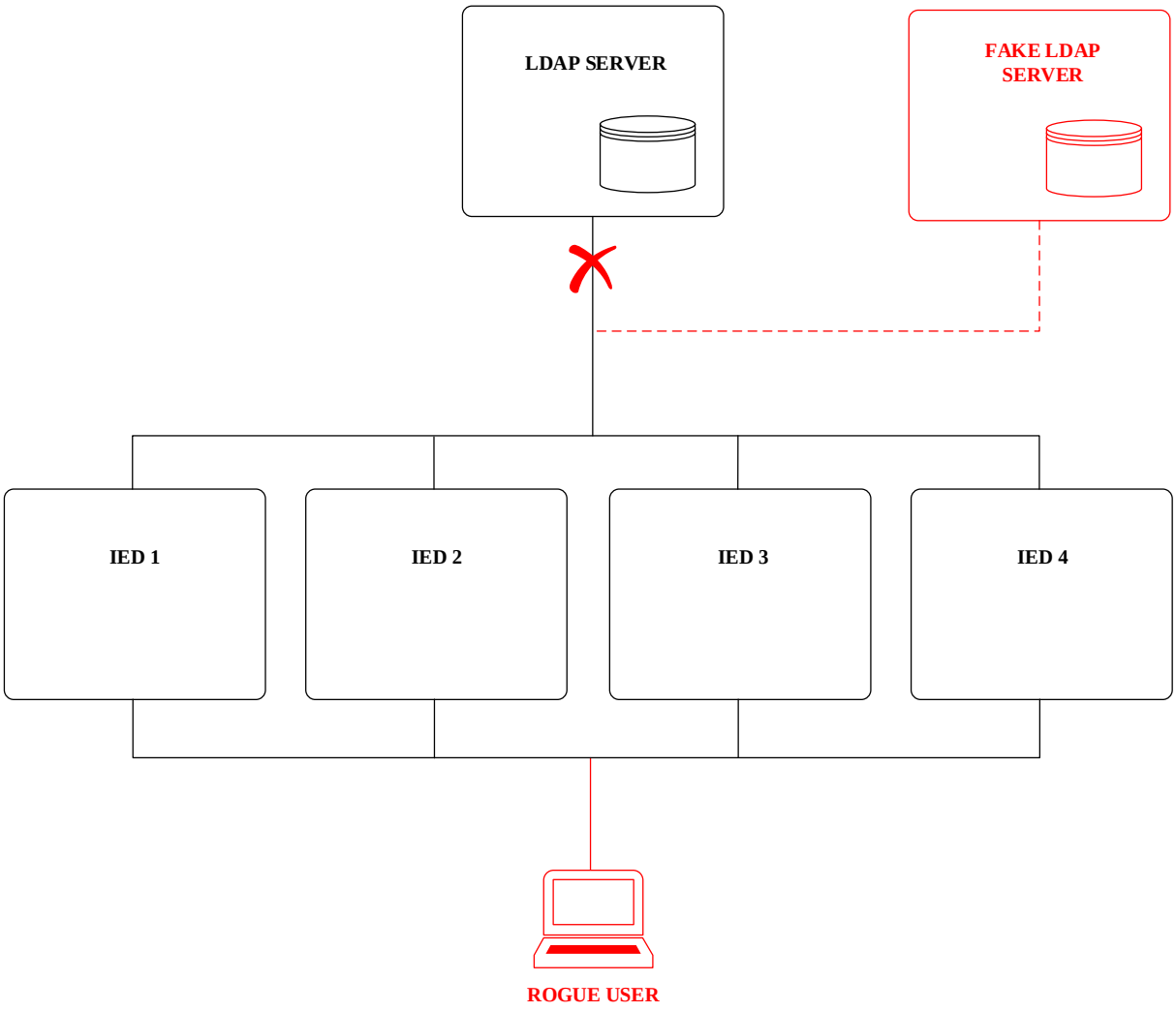

Figure 3.7.1 Fake LDAP server

In figure 3.7.1, a malicious user disguises itself as a LDAP server and responds to the IEDs request, for example with the same IP address as the valid server, therefore interfering between the correct LDAP server and with the communicating IED. The fake LDAP server then sends

its own list of users and roles to the IED, hence making the IED vulnerable because now a rogue user can access the IED with the credentials that the fake LDAP server has provided.

In order to avoid a situation where clients can be spoofed into believing that they are communicating with a valid server, certain authentication mechanisms should be used. As discussed before, LDAP supports TLS and client-server certificates. TLS is a security protocol that enables different applications to communicate with each other through a secure channel, and it can be used to protect important data from prying eyes [4]. As mentioned in IEC62351-8, TLS should be used to open a secure channel between the IED and the LDAP server [8]. Certificates should be used to prove the identity of the client and the server.

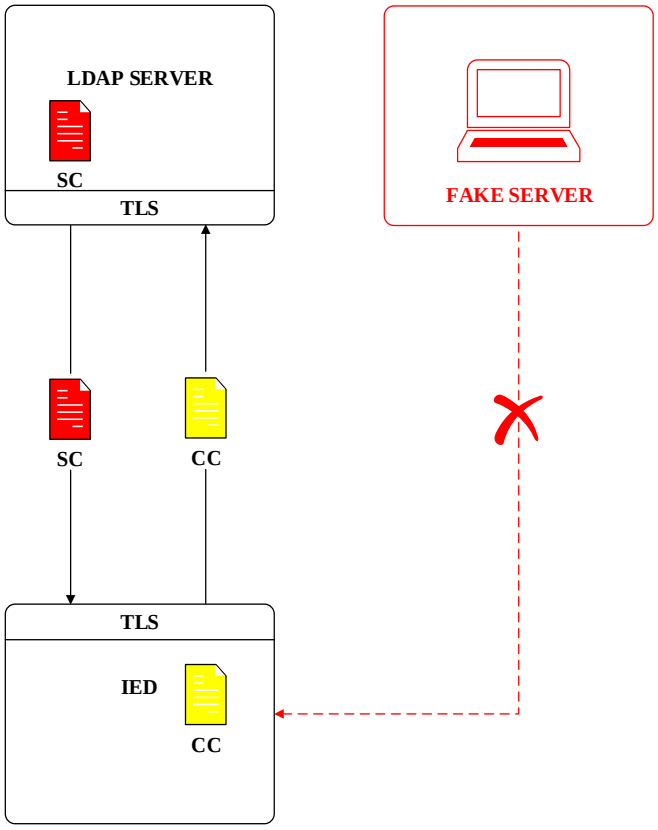

Figure 3.7.2 Client-server authentication

According to figure 3.7.2, when communicating to the LDAP server, TLS encrypted channel is opened and the LDAP server presents an SC to the IED that is signed by a trusted CA and the IED provides a CC that is signed by a trusted CA to the LDAP server to authenticate itself.

It must be noted that the receiver of the certificate can verify its validity by checking its signing CA and the validity date on the certificate (this process is explained in chapter 2.4). If the CA is unknown to the receiver, it can follow the trust chain until a trusted CA is found. If a trusted CA is not found then the certificate should not be accepted. When the client connects to the

server, it shall validate the SC presented during the verification procedure. To prevent spoofing it is important to add the IP address to the subject line of the SC and sign the certificate by the CA. By doing this, if a client connects to a fake server, the validation of the certificate will fail, and the connection won't be allowed.

3.8 Fake Client

Without proper client-server authentication, a fake client can harvest user names and possibly password information that can be used to log in to other devices in the substation network. Authentication is important because an attacker can manipulate the LDAP server to release sensitive information and with such concentration of data, security becomes very significant. Anyone who can take over the client-server connection can use the client's privileges to modify the data in the server.

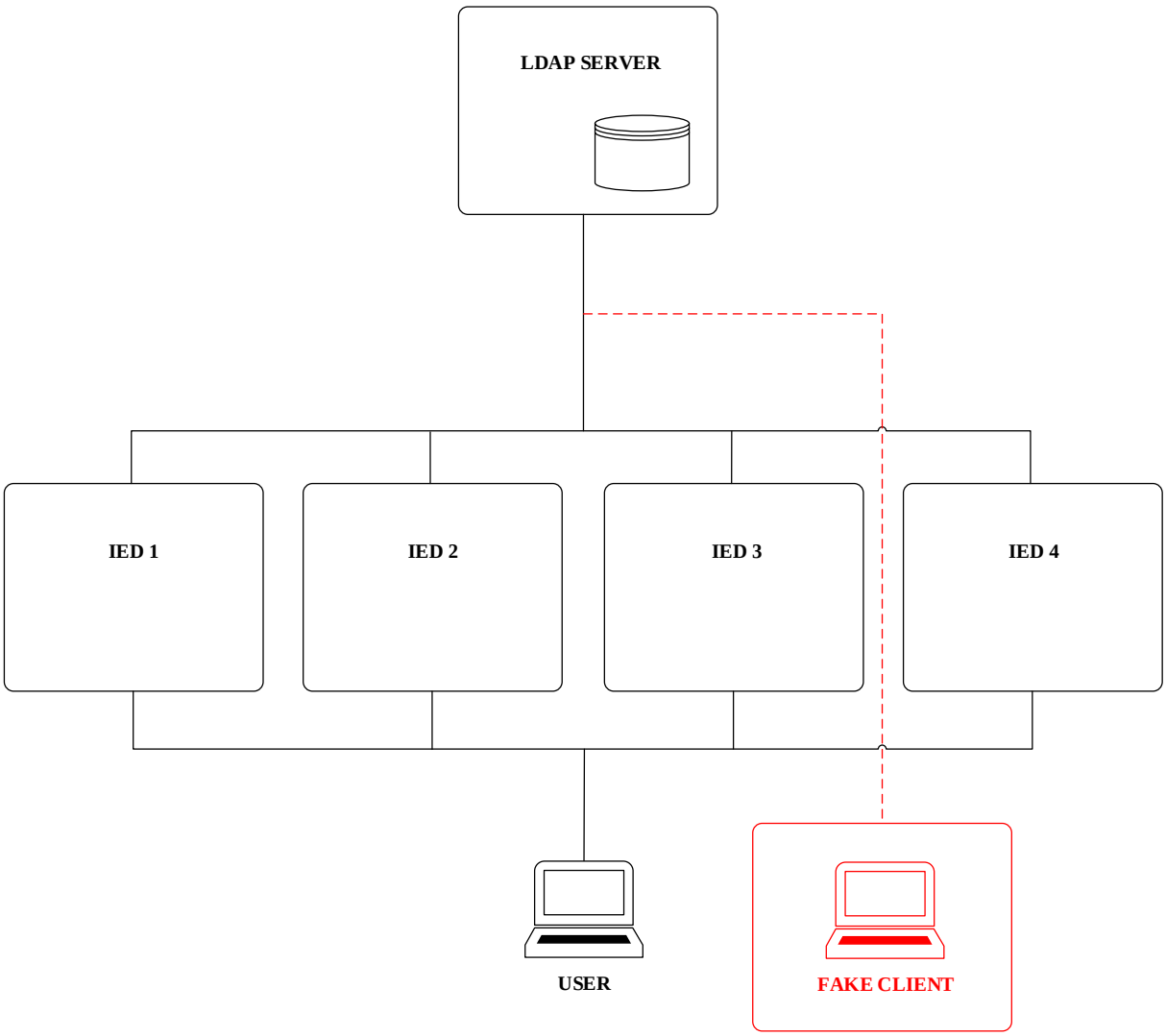

Figure 3.8.1 Fake LDAP client

In figure 3.8.1, a malicious user disguises itself as a client and sends a request to the LDAP server, for example with the same IP address as a valid client, therefore interfering between the correct LDAP server and with the communicating IED. If the fake client is able to communicate with the LDAP server, it can request the list of users and their roles, and later use it to access legitimate devices.

It is crucial to protect data inside the server and the client. In order to avoid a situation where the server can be spoofed to believing that they are communicating with a valid client, certain authentication mechanisms should be used. As discussed before, LDAP supports TLS and client-server certificates and as mentioned in IEC62351-8, TLS can be used to open a secure channel between the IED and the LDAP server [8].

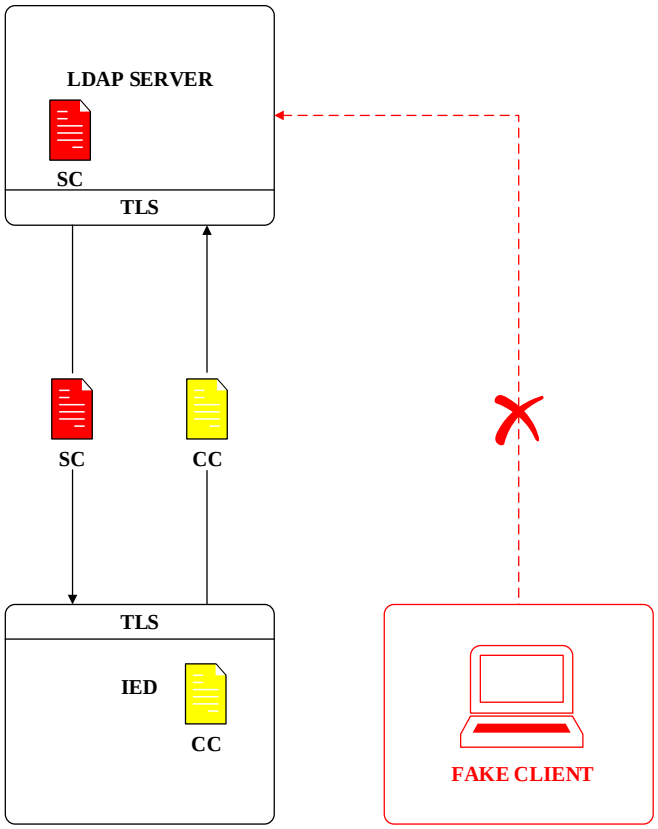

Figure 3.8.2 Client-server authentication

According to the figure 3.8.2, when the IED connects to the LDAP server, the LDAP server presents an SC to the IED that is signed by a trusted CA. The IED verifies the CA and the IED provides its CC to the LDAP server if requested. Exchanging certificates combined with TLS encryption creates security and confidence to both entities that the communicating devices are legitimate and the data transferred over the unsecured network is secured. It must be noted that the receiver of the certificate can verify its validity by checking its signing CA. If the CA is

unknown to the receiver, it can follow the trust chain until a trusted CA is found, if a trusted CA is not found then the certificate should not be accepted. When a fake client wants to connect to the server, then the server can request for a valid certificate. If a valid certificate, which is trusted by a recognized CA, is not presented then the connection will not be allowed.

3.9 Implementation proposal

As mentioned in chapter 2.5, the TLS protocol uses digital certificates to establish a secure communication channel between two connecting entities [17].

Using certificates and encryption protects and authenticates the communication between the centralized authentication server, the LDAP server, and the IED.

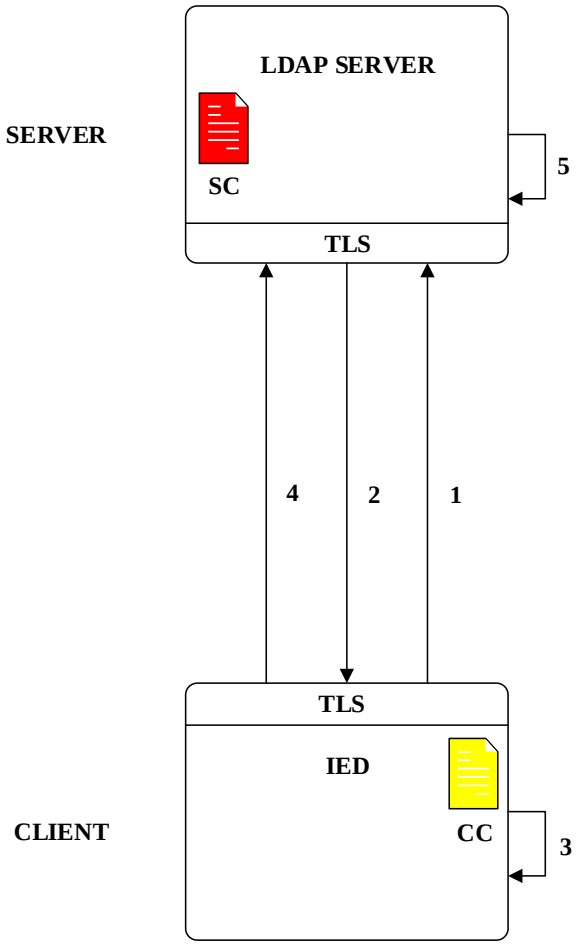

Figure 3.9.1 Certificate exchange between the LDAP server and the IED

The authentication process on figure 3.9.1 is as follows:

1. The IED sends a connect request to the server.
2. The server sends its SC, its asymmetric public key and requires a CC. It also provides a list of trusted CAs that the server accepts.

3. The IED validates the SC by checking its signing CA and by validating the CAs trust chain. It then creates a one of a kind symmetric key and encrypts it with the receiver's asymmetric public key.
4. The IED sends a CC based on the list of trusted CAs that the server has provided in step two, and it will send the encrypted symmetric key.
5. The server validates the CC by checking its signing CA or by validating the CAs trust chain and decrypts the symmetric key with its asymmetric private key.

After step five, the connection is now established as both entities have provided third party trusted certificates for authentication and they are in possession of the only two copies of the symmetric key that they can use to send encrypted messages to each other. The subset of the directory designated for that particular IED should now be replicated and stored into the IEDs local repository to have offline functionality.

As mentioned before, the motivation to use certificates is to provide trust in the network. Presenting a valid certificate that is trusted by a third party, the CA, provides assurance that the connected device is legitimate. The motivation to use encryption is to protect the transferred data, the user password, which is sent to the authentication server for verification. This solution combined with backup authentication servers for redundancy, local user list in the IED repository for local access in case of WAN loss, and user cache process to mitigate DoS provides security to the proposed system.

The critical issue with this proposal is that the IED does not have a secure storage option to store encryption keys securely. Although the information sent over the unsecure network can be made secure, information on the IEDs memory can be stolen. It is important to protect encryption keys that are stored on the device. Another issue is that the connection between the IED and a connecting client is unsecure. Current proposal has focused on the security between the IED and the authentication server but the following chapter focuses on the security between a client and the IED as a server. It also focuses on the secure storage problem.

4 Hardware Root of Trust

4.1 Overview

In order to generate trust between the client and the server, both participants need to have the ability to provide proof of their trustworthiness. This can be done using a trusted third party who verifies the credibility of the device. As discussed in chapter three, the IED and the centralized authentication server have to open a TLS protected connection and use client-server certificates as proof of trustworthiness in order to exchange data in a secure manner. But what happens when a client, an engineer on a separate platform, connects to the server IED? With the current system, the IED does not provide proof to the client if it is a trusted entity. An attacker can masquerade as an IED and steal password information from the connecting entity in order to use it later to connect to a legitimate substation device. For the connection to be secure, both the client and the server should have third party trusted certificates for authentication and the connection between the participants should be protected using TLS encryption.

The IED can be equipped with a SC, delivered at the same time as the CC that is used to connect to the centralized authentication server, the LDAP server. Both of the certificates have to be signed by a trusted third party, the CA. The proposed system uses IP address in the certificate subject to prove that the SC belongs to the server that was connected to in order to prevent IP address spoofing. The problem with this approach is that when changes are made to the IEDs IP address, a new SC has to be created. There are two possible options to replace certificates. The first option is that an engineer creates a new SC, using a trusted CA tool, and transfers the certificate and the asymmetric key pair to the IED manually. In a system with thousands of IEDs, this method can be quite troublesome and take days if not weeks to finish. The second option is to use auto enrollment, meaning that the IED sends a request to a trusted CA in order to get a new SC when the previous certificate becomes invalid due to any changes to the IED settings. This approach creates a major security problem as transferring the SC and the asymmetric key pair over the network is dangerous due to the fact that an attacker can steal the data and use it to impersonate a valid IED, and therefore be able to harvest password information from the connecting entities. Therefore the request to the CA from the IED should be done using the CC to authenticate and the connection needs to be encrypted to protect the transfer of encryption keys. The issue here is that when the SC becomes invalid due to an IP

address change, then what happens if the CA is offline? As availability is critical in a substation environment then an alternative solution is needed otherwise the IED can't be connected to.

A possible solution is that the IED can have the ability to generate and sign its own SC. As self-signed certificates provide little or no trust in the substation network, then a more viable option should be used. A SC, which is signed by a valid CA, can be trusted, but this would mean that the CA has to be saved onto the IEDs internal memory in order to create a new SC when any changes are done to the device that directly affect the information in the SC. Having a CA on the IED creates a new security risk as information in the device is often stored in an unencrypted form on the internal memory that can be removed from the device itself. What happens if the signing key of the CA is leaked? An attacker could use it to sign a SC for a fake server and harvest information from the client.

In order to prevent the signing key of the CA getting into the wrong hands, it has to be stored safely. As each IED has some sort of internal memory, either a flash card or a memory chip to store data, then the signing key of the CA could be stored in an encrypted form. In order to minimize risk, an I-CA should be used instead of the R-CA, as the R-CA is needed to be kept safe and its signing key should be kept a secret at all cost. If the R-CA is compromised, then all CAs that rely on it are affected. Therefore, even when the I-CAs signing key gets compromised, this will not affect the credibility of the R-CA.

Storing the I-CAs signing key on the IEDs internal memory creates a new problem. Because the internal memory can be removed and the secret data can possibly be decrypted, a more secure option should be considered. This is where secure storage comes in. A TPM can be used to provide that extra security to store cryptographic keys including the symmetric key, asymmetric private key and the signing key of the I-CA.

Because TPMs security is hardware not software based, systems containing it can be made to be trusted. TPM can provide protection in computation as the encryption, decryption, and signing process is done inside the TPM. This protects the keys from being stored on the local memory bus or on the Random Access Memory (RAM) where they can be snooped. It also mitigates the risk of losing the keys during transit, meaning that transferring keys from one location to another can be avoided as the installment of keys can be done in the factory either where the IED is made or it can be done by the manufacturer of the chip. [19]

4.2 Trusted Platform Module

TPMs are used as hardware root of trust in many enterprises, and it is a specialized memory chip that is used to store encryption keys safely. It provides hardware based approach for security instead of software based security that is regularly defeated. [20]

A TPM is therefore a memory module that can be used to provide secure storage and that functionality is missing in the current system.

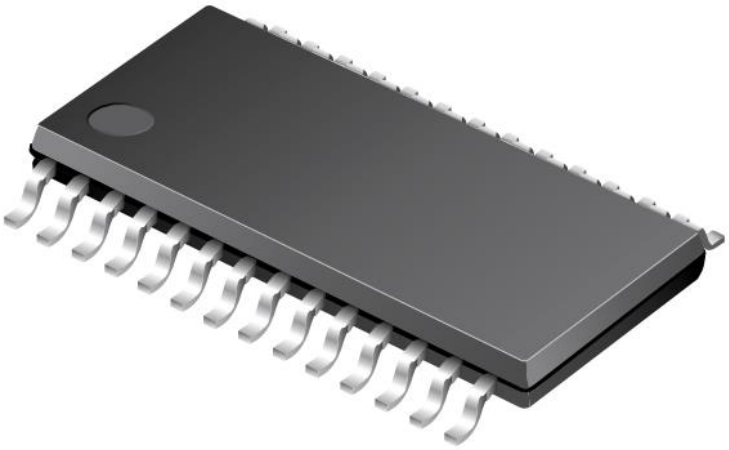

Figure 4.2.1 Trusted Platform Module (TPM) [21]

As seen on figure 4.2.1, TPM is an Integrated Circuit (IC) that is attached to the motherboard of the platform it is meant to authenticate and it contains built in memory and logic for certain activities like encryption, platform monitoring, and secure data storage. [22]

Therefore, adding the TPM on the IEDs motherboard and storing the encryption keys on the chip can be the solution for providing secure storage. As noted in chapter 3.8, when a compromised client connects to the network, then the security of the whole system is undermined. Software authentication methods can be bypassed and in order to verify that the IEDs have not been compromised by any unauthorized modifications, it is important to monitor how they are configured and what processes are running on the platforms. Therefore it is important to verify that no one has tampered with the device.

In order to check that no unauthorized person has tampered with the hardware and software, it is important to [20]:

- *Measure firmware, software and configuration data before it is executed.*
- *Store those measurements in a hardware root of trust, like a TPM.*

- *Validate that the measurements made actually match the measurements that were expected*. [20]

Systems containing TPMs can be scanned at boot for signs of change and attest to whether or not the machine meets security requirements before the boot is executed [22]. Therefore, having obtained an integrity metric for the platform during the boot process, the results can be stored in the TPM and compared against every boot sequence in order to verify that no unauthorized modifications have been done.

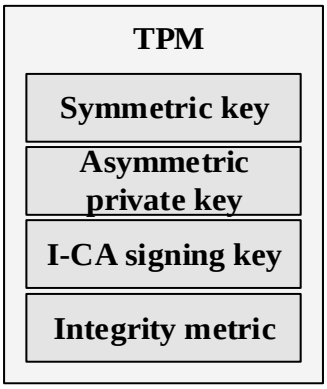

Figure 4.2.2 Using TPM to store sensitive information

As shown on figure 4.2.2, the TPM can be used to store encryption keys and the integrity metric safely in order to protect sensitive information. As mentioned in chapter 3.5, in case of connection loss, the IED needs to have a local list of users, passwords and roles in its internal memory in order for the device to be accessed by the designated users while it is offline and not connected to the authentication server. This information, which is stored on the IEDs internal memory, can be encrypted using the TPMs cryptographic capabilities and the signing key can be saved securely on the chip. *The TPM uses a specialized key to encrypt and decrypt data and once it is burned onto the chip, it never leaves the TPM and it provides the root of trust* [23]. Therefore, access to data is controlled by a cryptographic key and it can't be decrypted when the internal memory is removed as the necessary key is stored securely on the TPM. Only the device containing the TPM and the necessary key can therefore decrypt the information. Using the encrypted data on the memory module can be connected to the integrity measurement of the device, meaning that the data can only be decrypted when the device has been verified safe [22]. A TPM should be used to enhance IEDs security and it can provide secure storage for cryptographic keys including the signing private key of the I-CA. Information on the internal memory, for example the user list, can be encrypted and decrypted only when the IED is considered safe by comparing integrity metrics.

4.3 Implementation Proposal

For the IED to have the ability to create and sign its own SC by a trusted third party, the I-CA, it needs to have its signing private key, that provides trust to the certificate, stored securely on the TPM. It is important to protect the signing key of the I-CA, otherwise any attacker could steal it and create and sign its own certificate and act as a legitimate entity in the network. When any changes are done to the IEDs IP address, the I-CA needs to generate a new SC and sign it with its private signing key. The SC is used to authenticate the IED as a legitimate server to the connecting client. The I-CA could be stored on the IEDs internal memory, but for added security, its signing key should be stored on the TPM. As noted in chapter 4.1, certificate signing can be done inside the TPM, this means that the signing key never leaves the chip, therefore it is protected against being snooped from the local memory bus or RAM.

When the IED is booted up the first time or when the IP address is changed, the I-CA using its signing private key (on figure 4.3.1 it is marked as PK), that is stored on the TPM, needs to generate and sign a new SC in order to authenticate the IED to the connecting client in the network. When the IEDs IP address is changed, then a new SC is generated and signed by the I-CA. This process has to be followed every time when changes are done to the IED that affects the information in the SC.

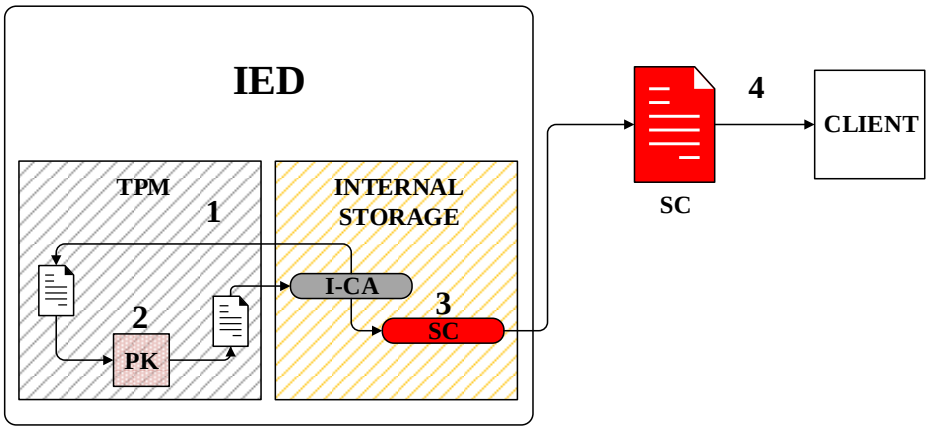

Figure 4.3.1 IED with secure storage and the I-CA (PK on the TPM)

The process is as following:

1. The I-CA generates an SC and sends it to the TPM to be signed.
2. The certificate is signed with the private signing key (PK) of the I-CA that is stored on the TPM.
3. Signed certificate is stored on the IEDs internal memory.

4. During the authentication process, the SC is provided to the client.

Now that the SC is signed by a trusted entity, the certificate can be presented to a connecting client therefore providing proof that the IED is a valid server, not an entity that is trying to harvest information. This solution, combined with TLS encryption can protect the communication between the IED and the connecting client. Therefore, the connection between the connecting client, an engineer's laptop for example, and the IED as the server can be performed as on figure 4.3.2.

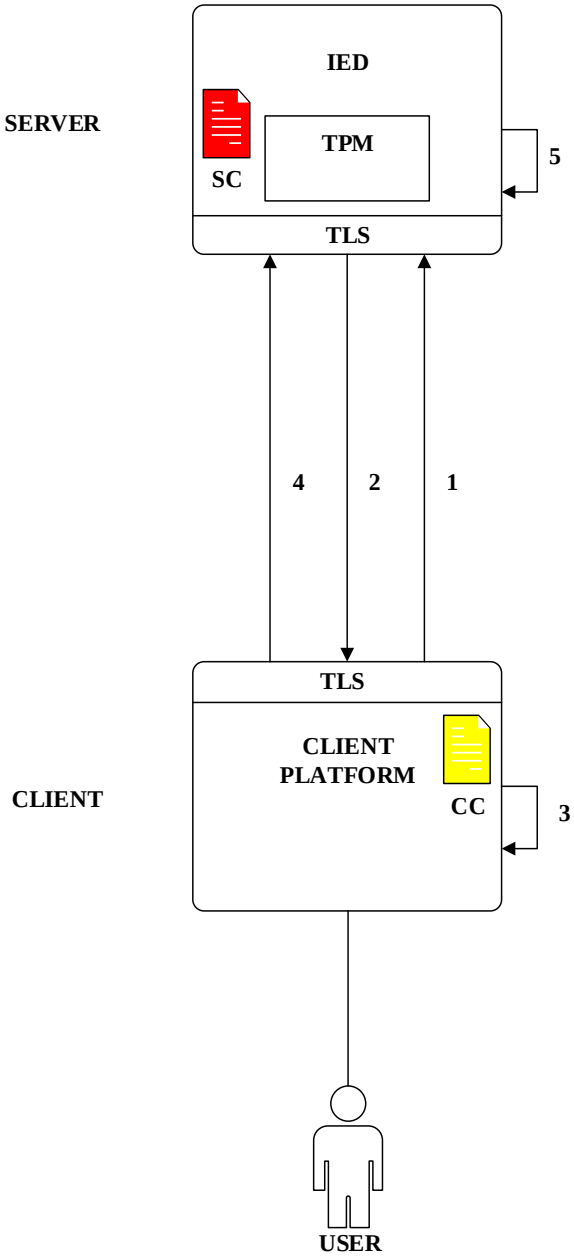

Figure 4.3.2 Implementation proposal for IED as a server

According to figure 4.3.2, in order to connect to the IED, the client should have its CC installed that is generated and signed by a trusted CA. The verification process is as following:

1. The client sends a connect request to the server IED.
2. The server IED sends its SC and its asymmetric public key. It also requires a CC from the connecting client and provides a list of trusted CAs that the server accepts.
3. The client validates the IEDs SC by checking its signing CA or by validating the CAs trust chain. It generates a one of a kind symmetric key and encrypts it with the IEDs asymmetric public key.
4. The client sends a CC, based on the list of trusted CAs that the server has provided in step two, and sends the encrypted symmetric key to the IED.
5. The server IED validates the CC by checking its signing CA or by validating the CAs trust chain, and decrypts the encrypted symmetric key with its asymmetric private key.

Now that step five is done, both entities have the only two copies of the symmetric key that they will use to encrypt messages and therefore the information sent over the network is now protected by TLS encryption that was explained in chapter 2.5. As both parties have provided third party trusted certificates for authentication then this solution can give both sides the confidence that they are talking to a trusted entity. Now that a secure channel has been opened, the user can send its username and password over to the IED to be verified. If the IED is online, then it will request the LDAP server to verify it but if it is offline then the internal list will be used to compare the input and to assign the role to the user.

In order to generate trust in the network, it is important that all entities have trusted third party signed certificates installed, giving a possibility to authenticate each and every platform. IEDs that have the secure storage capability option, should also have the possibility to create and sign their SC when information is changed that directly affects the existing SC. With this approach, all devices in the substation network can be made secure.

Users who need to connect their platform, for example an engineer’s laptop, to the IED, need to request a CC from a trusted CA. A system administrator can be in charge of the CA tool and assign who and from which device is allowed to access the IED. This would allow the utility to have full control over who can connect to its IEDs. A possible verification process solution is shown on figure 4.3.3.

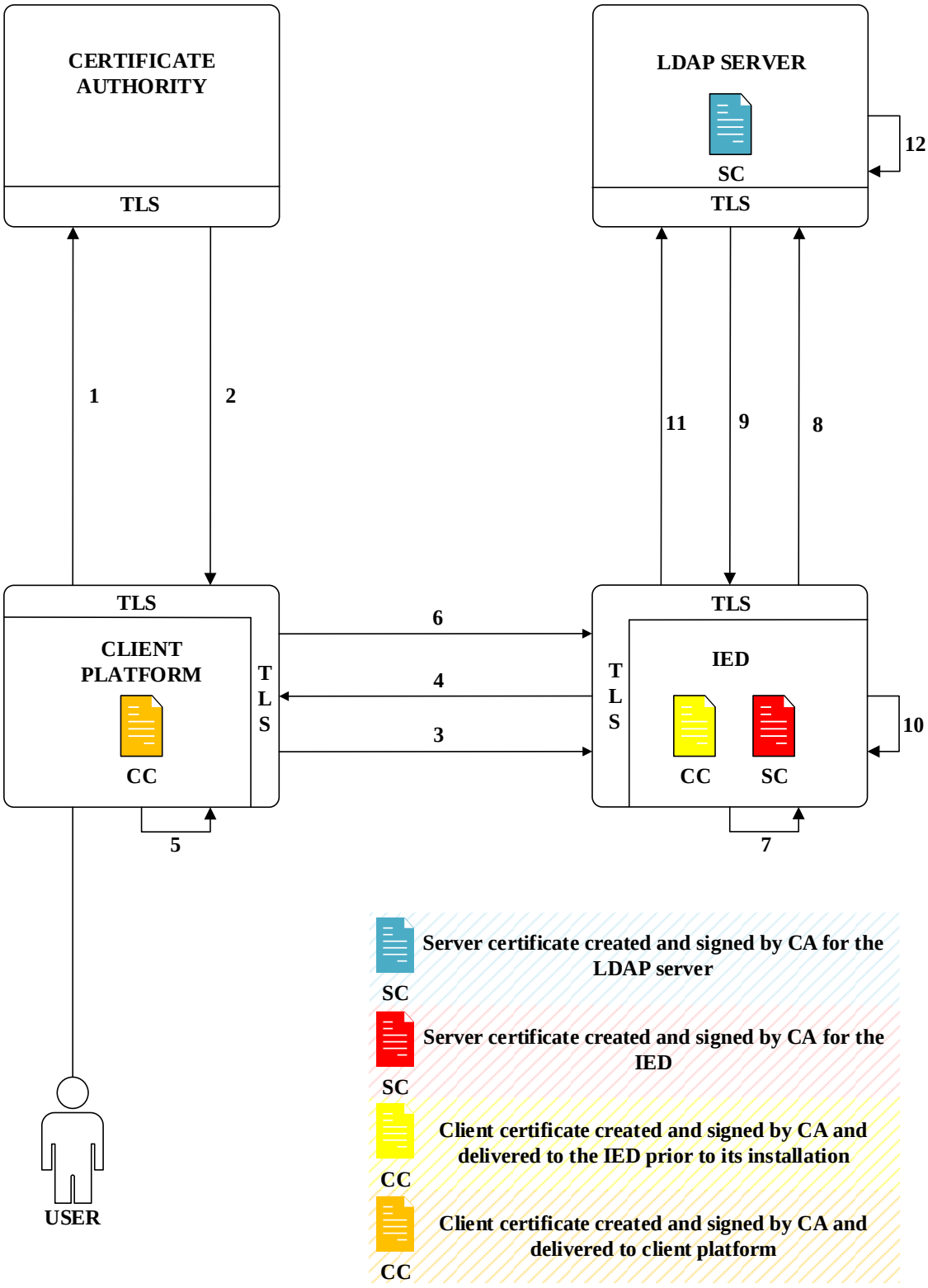

Figure 4.3.3 Complete verification process

The TLS protected connection should be opened between each connecting entity in order to protect information sent over the network. Note that the exchanging of cryptographic keys is

not mentioned to simplify explaining the certificate exchange process. The process in figure 4.3.3 is as follows:

1. The user on the client platform requests the CA for a CC in order to connect to the IED.
2. The CA authenticates the user and sends the CC to the client platform.
3. The client platform sends a connect request to the server IED.
4. The server IED sends its SC and requires a CC. It also provides a list of trusted CAs that the server accepts.
5. The client platform validates the IEDs SC by checking its signing CA or by validating the CAs trust chain.
6. The client platform sends a CC based on the list of trusted CAs that the server has provided in step three.
7. The server IED validates the CC by checking its signing CA or by validating the CAs trust chain.
8. The client, that is now the IED, sends a connect request to the LDAP server.
9. The LDAP server sends its SC and requires a CC from the IED. It also provides a list of trusted CAs that the server accepts.
10. The IED validates the SC by checking its signing CA or by validating the CAs trust chain.
11. The IED sends a CC based on the list of trusted CAs that the LDAP server has provided in step nine.
12. The LDAP server validates the IEDs CC by checking its signing CA or by validating the CAs trust chain.

After the validation process, the user enters his/her credentials and the IED validates them via LDAP server and receives the roles. The user can now access the IED and perform activities according to his/her role. This solution gives full control to the utility and authenticates each entity.

4.4 Certificate Handling

Introducing a system that uses certificates for authentication creates a need for a scheme that can be used to manage them. Certificates can be issued with an expiration date, but sometimes there are situations when certificates need to be revoked before that date has passed.

A certificate revocation is the act of invalidating the certificate before it expires. A certificate should be revoked when the private key of the CA or the certificate holder is compromised,

when the purpose for the certificate does not exist anymore or when the holder of the certificate is not trustworthy anymore. [3]

It is therefore important for the integrity of the certificate management system to verify the validity of certificates. In a substation automation system, a possible method to handle certificate revocation is to use CRLs.

A CRL is a list of serial numbers of certificates that have been revoked by the issuing CA. The receiver of the certificate can check its validity by comparing the serial number against the CRL. If a match is found then the certificate should not be accepted. The list is time stamped and renewed after a specific interval. [19]

Therefore, every certificate should have a specific lifespan and a serial number and if during the lifespan the certificate has to be revoked, then the certificate serial number is placed on the CRL and sent to the clients. The certificate should be in the list until its validity date has passed as the certificate that is expired is not accepted by the receiver anyway, then there is no reason why it should be kept in the list. Using CRLs can be one of the solutions to manage certificates but there is a significant problem with using them. They do not operate in real-time as the list is downloaded by the IED after a specific time period, therefore the list inside the IED is updated when the new CRL becomes available or the cached one expires [19].

It is necessary to use a method to receive the latest revocation announcements. A possible solution is to use the OCSP. OCSP allows the IED and the centralized authentication server, the LDAP server, to send real-time requests to the service and check the status of the certificate. In an online mode, the IED receiving a CC can verify its status by transmitting a query to the OCSP server with the serial number of the certificate to see if it has been revoked instead of relying on its copy of the CRL. [24]

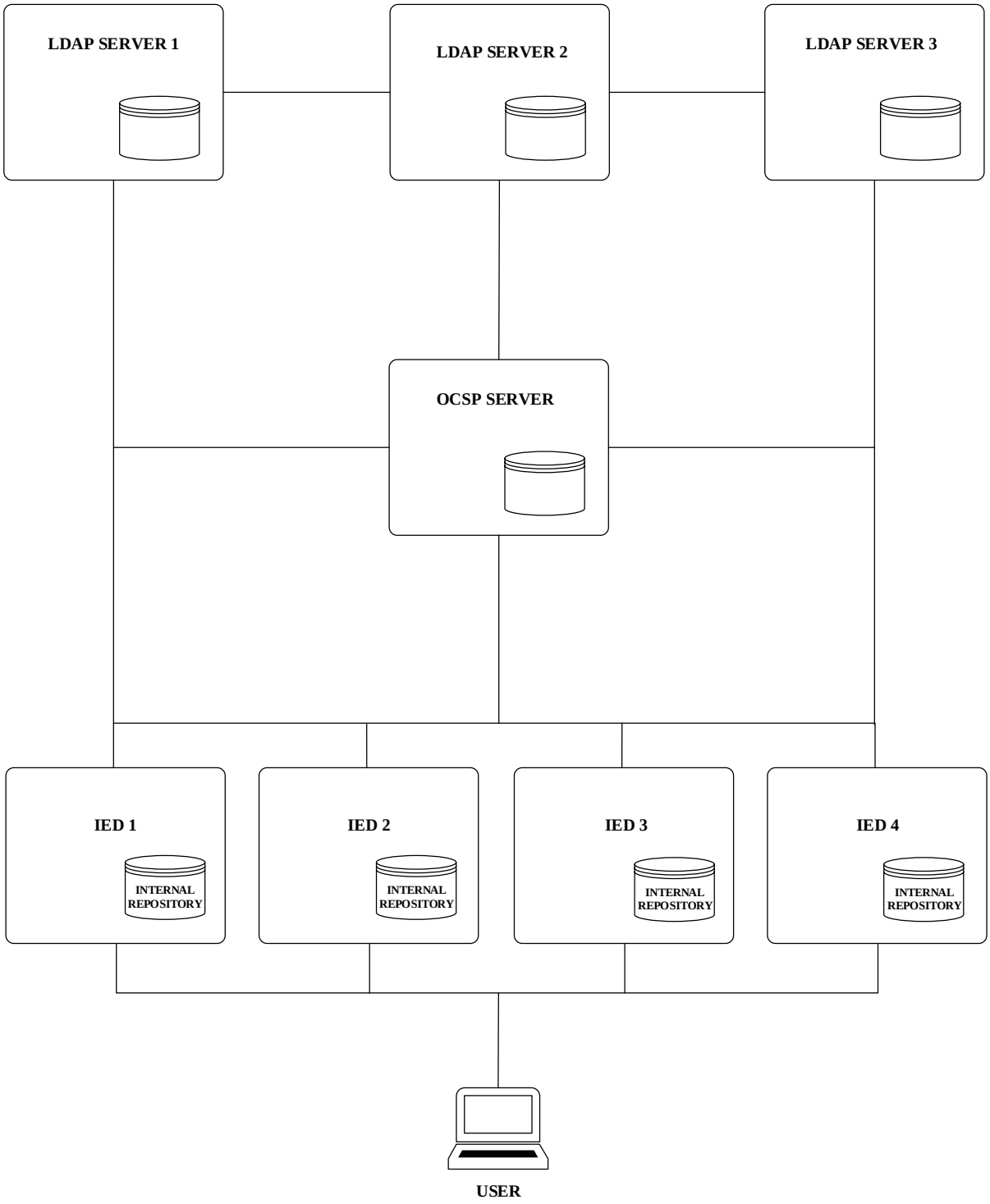

Figure 4.4.1 Certificate handling with OCSP server

A combined solution should be used in order for the IED to work both in online mode and offline mode. According to the figure 4.4.1, checking the revocation status from the OCSP server when the IED is in online mode, and in case of connection loss to the centralized authentication server, the LDAP server, the IED should have the CRL in its internal repository. Only then can the proposed system work correctly, otherwise users will be locked out from the

IEDs when the centralized authentication server, the LDAP server, is offline. In order to consume less bandwidth, the CRL should be downloaded only after a specific time or only when the CA releases the latest CRL. Whenever a newer version of the CRL is released by the CA, the existing CRL should be overwritten in order to consume less space in the IEDs internal memory. In order to provide security, the communication between the OCSP server and the IED, and between the OCSP server and the LDAP server, should be protected by TLS encryption. The server should be fully secure and tamper resistant in order to prevent unauthorized modification of information.

The centralized authentication server, the LDAP server, should verify that the CC, that it is received from the IED, is still valid by checking its expiration date and comparing its serial number against the CRL, when the OCSP server is offline, or when it is online, requesting the verification directly from the OCSP server.

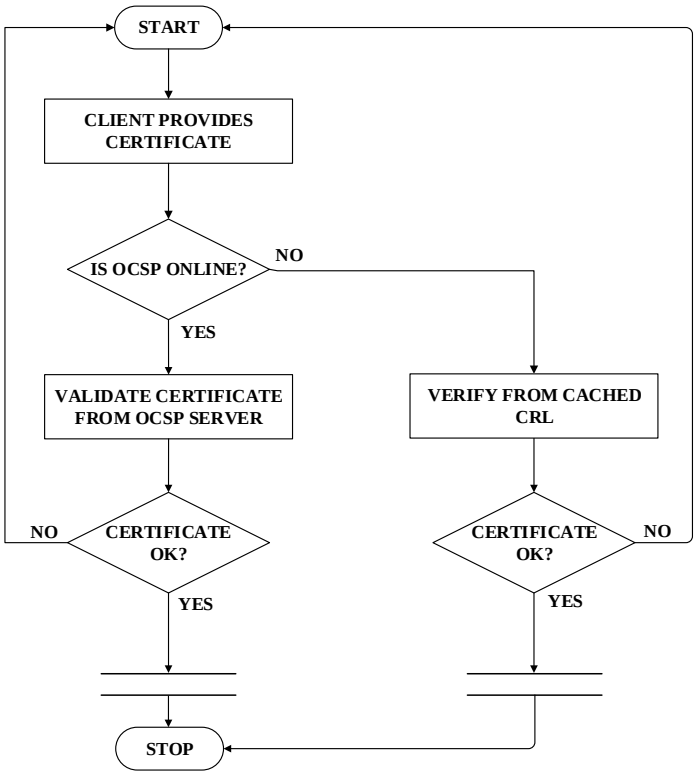

Figure 4.4.2 Logic diagram for certificate verification

The logic diagram on figure 4.4.2 describes the certificate validation process. When the OCSP server is online, the certificate verification is done using the OCSP server. When the OCSP server is offline, then the receiver of the certificate will check its serial number using the cached CRL.

Conclusion

This study set out to explore the implications of adding a centralized user account management system into a substation automation environment, to identify the dangers that affect the system, and to propose solutions to improve the security status.

The problems that were defined were unsecured connections between devices and no validation of identity, creating possibilities for spoofing. This combined with a risk of SPOF and a DoS created a need to improve on security. The proposed system can be protected or at least the threats can be mitigated by using the principles of redundancy, security measures, and authentication. Creating a system where information sent over the network is encrypted and trusted third party signed certificates are exchanged, can provide confidence that the connected entities are legitimate. In order to provide security during transit, encryption between the IED as the client and the authentication server has to be established to protect sensitive user information from being stolen when it is transferred over the unsecured network to the centralized authentication server for verification.

In order to protect the communication and to identify each participant when a client platform connects to the server IED, it is important to use certificates for authentication. The IED can be equipped with an SC in order to authenticate itself to the connecting client. During the analysis, a new obstacle was identified. Because the SC contains specific information about the server IED, altering its settings, such as changing the IP address (that is in the subject of the certificate in order to prevent IP address spoofing), causes the SC to become invalid. Therefore a new SC is needed. Due to time constraints and in order to improve efficiency, an I-CA can be installed on the IED in order to create a new SC when needed. Due to the unsecure nature of the IEDs internal storage, encryption keys (symmetric, asymmetric private key, and the private signing key of the I-CA) can’t be stored safely because the internal memory can be taken out of the device and data can be removed from the memory. Because current IEDs do not have a secure storage option for encryption keys then the proposed centralized authentication system can be at risk as the keys in the IED can be stolen and used to harvest information as a valid entity. Due to the problem with the IED lacking secure storage, the author recommends using a TPM for storing encryption keys safely in order to protect the proposed certificate infrastructure in substation automation systems. An added benefit with the TPM is that signing an SC can be done without the key leaving the chip therefore it can’t be snooped from the local memory bus or RAM.

As TPM can provide the necessary security, hardware root of trust can be implemented. Therefore, the system is moving from trusting software to trusting hardware. As software can be modified more easily, trusting hardware like the TPM, can be a possible way forward in security engineering. This can be of significant value in markets where cyber-security is the top priority, this particular solution can provide more opportunities for IED vendors. The proposal fills the gaps in research that currently hasn't focused on the security between the IED and the client, and the secure storage problem in substation automation devices.

Using client-server certificates creates a need to manage them in a substation automation environment, therefore a possible solution is to use CRL for offline use and OCSP servers for online certificate management. The proposed certificate management solution provides the redundancy in case the connection to the centralized authentication server is lost with locally stored CRLs and during online operations real-time certificate status checks can be performed by requesting the certificate verification from the OCSP server.

The summary of major findings and recommendations based on this analysis:

- Backup centralized authentication servers can provide redundancy for the system and the user information can be replicated between servers.
- Offline functionality is needed in case of connection loss to the centralized authentication server in order to access the IED. This can be achieved by storing a user list in the local repository of the IED. It must be noted that the list of users and passwords should be encrypted in order to protect the information.
- Encryption between the IED as the client, and the authentication server has to be established to protect sensitive user information when it is being transferred to the server for verification.
- Encryption between the IED as the server, and the connecting client should be used to protect sensitive user information when it is being transferred to the server for verification.
- In order to identify each connecting entity, it is crucial that each device has trusted third party signed certificates installed that provide proof that the devices are legitimate.
- In order to protect the cryptographic keys, a secure storage option should be installed on the IED. A TPM is recommended.
- A CA can be installed on the IED in order to create a new SC when the IP address is changed, and its signing private key should be stored on the TPM.

- An I-CA should be installed instead of the R-CA to protect the certificate infrastructure.
- Real-time certificate status checking can be achieved by using an OCSP server and for offline functionality, locally stored CRL should be used.
- For full control, every client should have a CC to authenticate itself and every connected entity should be able to provide an SC in order to provide proof that they are legitimate.
- Monitoring the hardware configuration and the running software stacks on the IED can be connected to the TPM by storing an integrity metric on the module and verifying the running processes against the metric.

Implementing full control and authentication, as proposed in chapter 4.3, can be difficult to achieve as the proposed system creates more work and a need to request a certificate from the CA prior to connecting to the IED. A possible way to improve user accessibility is to only use an encrypted connection between the client platform and the IED but during the handshake procedure, only the IEDs SC is presented. There is a loss in security as the client platform can't be authenticated but there are gains in user accessibility.

Future work could concentrate on implementing a single corporate account based logon into all the systems to which the user is granted access, therefore creating the possibility to authenticate once on a platform that is trusted, and connecting that platform to devices that are safe to connect to, creating platform to platform trust. It is still unclear how to solve the secure storage problem with legacy devices that do not have that particular capability. Possibly, encrypting the internal memory could be used in order to safely store the encryption keys. Another area to look into is using platform monitoring to verify that no software and hardware modifications have been made on the IED without the owner's consent. Additional information is needed about performing field modifications and repairs on IEDs when platform monitoring is implemented and the IEDs conditional state is connected to the integrity metric on the TPM. In order to protect the substation from a DoS, automatically disabling a communication node to the IED can possibly be implemented, more research is therefore needed.

Based on this research, implementing a relatively safe centralized authentication system in a substation automation environment is possible when security requirements, like encryption and client-server certificates and secure storage, are introduced. In order to adequately secure the system, it is important to use technical solutions that can provide the necessary security but eventually, the security solutions used are ultimately a business decision based on a number of specific requirements and standards that vary from region to region. This thesis tries to create awareness and inform the reader about the dangers that affect substation automation devices

that are considered critical assets. After researching this subject, the author has come to the realization that due to the strategic nature of the energy system and its infrastructure, security should be integrated directly into each individual device in order to make the substation automation system more secure as a whole.

References

[1] H. F. Tipton and M. Krause, Information Security Management Handbook, 2006.

[2] J.-L. P. Jacques Benoit, *Making the most of substation IEDs in a secure, NERC compliant manner,* 2006.

[3] M. Mahmoud, J. Misic and X. Shen, *Efficient Public-Key Certificate Revocation Schemes for Smart Grid,* 2013.

[4] A. Findlay, *Best Practices in LDAP Security,* 2011.

[5] International Electrotechnical Commission (IEC), *IEC62351-10 Power systems management and associated information exchange- Data and communications security- Part 10: Security architecture guidelines,* 2012.

[6] D. Thanos, "Cyber Security of Substation Control and Diagnostic Systems," in *The Electric Power Engineering Handbook,* 2012, pp. 17-1 to 17-28.

[7] S. Kunsman and M. Braendle, *Cyber Security for Substation Automation, Protection and Control Systems,* 2010.

[8] International Electrotechnical Commission (IEC), *IEC 62351-8 Power systems management and associated information exchange- Data and communications security- Part 8: Role-based access control,* 2011.

[9] M. G. Seewald, *Multi-layer security architecture for electrical substations,* 2013.

[10] ABB Switzerland, 2009. [Online]. Available: http://new.abb.com/docs/librariesprovider101/default-document-library/1kha001069-sen-substation-automation-solutions-sas-600-series.pdf. [Accessed 06 01 2015].

[11] The North American Electric Reliablity Corporation (NERC), *Standard CIP-004-3a- Cyber Security- Personnel and Training,* 2006.

[12] D. Boneh, "Cryptography I," 2014. [Online]. Available: https://class.coursera.org/crypto-010/lecture/preview. [Accessed 06 01 2015].

[13] International Electrotechnical Commission (IEC), *IEC 62351-2 Power systems management and associated information exchange- Data and communications security- Part 2: Glossary of terms,* 2008.

[14] Citrix, "Citrix Product Documentation," 2014. [Online]. Available: http://support.citrix.com/proddocs/topic/xenapp5fp-w2k8/sg-cryptography-types.html. [Accessed 05 01 2015].

[15] D. R. Kuhn, V. C. Hu, W. T. Polk and S.-J. Chang, *Introduction to Public Key Technology and the Federal PKI Infrastructure,* 2001.

[16] Entrust, *The Concept of Trust in Network Security,* 2000.

[17] Entrust, *Understanding Digital Certificates & Secure Sockets Layer,* 2007.

[18] A. Findlay, "Security with LDAP," 2002. [Online]. Available: http://www.skills-1st.co.uk/papers/security-with-ldap-jan-2002/security-with-ldap.html. [Accessed 05 01 2015].

[19] E. Turkaly, *Securing Certificate Revocation List Infrastructures,* 2001.

[20] G. Shpantzer, *Implementing Hardware Root of Trust: The Trusted Platform Module Comes of Age,* 2013.

[21] J. D. Osborn and D. C. Challener, *Trusted Platform Module Evolution,* 2013.

[22] P. E. Sevinc, D. Basin and M. Strasser, *Securing the Distribution and Storage of Secrets with Trusted Platform Modules,* 2007.

[23] D. Dorwin, *Cryptographic Features of the Trusted Platform Module,* 2006.

[24] Cisco Systems, *Public Key Infrastructure Certificate Revocation List Versus Online Certificate Status Protocol,* 2004.