

White Paper: Cybercom Enhanced Security Platform

There is a wide range of systems where the assurance of the confidentiality, integrity and availability of the applications and data is of great importance. One way of achieving this is to keep all applications in a closed network environment. However, the expanding demand for service oriented applications increases the need for opening up these systems for interaction with external users and services. At the same time it is important that the communication with the internal applications does not put the integrity, confidentiality and availability of the system at risk in any way.

Cybercom Enhanced Security Platform adds a security layer to a closed network environment which enables efficient and effective interaction without compromising the integrity and confidentiality of the system.

Table of Contents

1	Executive Summary	5
1.1	The solution	5
1.2	Result	5
2	Background	6
3	Overall Requirements	7
3.1	Security	7
3.1.1	<i>Availability</i>	7
3.1.2	<i>Confidentiality</i>	7
3.1.3	<i>Data Integrity</i>	7
3.1.4	<i>Non-repudiation</i>	7
3.2	Performance	7
3.3	Scalability	7
3.4	Flexibility	8
3.5	Monitoring and Logging	8
3.6	Interoperability	8
4	Platform Overview	9
5	Technical Description	11
5.1	Authentication using CESP-ID	11
5.1.1	<i>CESP-ID in detail</i>	11
5.1.2	<i>Services</i>	11
5.2	Access Control using CESP-Access	12
5.2.1	<i>Authorization Process using Axiomatic Policy Server (APS)</i>	12
5.3	Logging using CESP-Log	13
5.4	Control and Audit using CESP-Analyzer	14
5.4.1	<i>Analysis Process</i>	14
5.4.2	<i>Reporting</i>	15
5.5	Secure Communication with CESP-Link	15
5.6	Server Management with CESP-Admin	16
5.7	Notification by CESP-Notify	17
5.7.1	<i>Notification procedure</i>	18
5.7.2	<i>CESP-Notify components</i>	18
6	Conclusion	19

Copyright: © Cybercom Sweden East AB 2009. All right reserved

Disclaimer: No part of this document may be reproduced in any form without the written permission of the copyright owner.

Cybercom reserves the right to change the specifications at any time and without notice. Cybercom shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademarks: All trademarks or trade names are the property of their respective owners.

1 Executive Summary

There are a large number of systems where the confidentiality, integrity and availability of the applications and data are of great importance. Typically, this can be assured by implementing the system within a closed network environment with no or very limited access to applications and data for external users. However, the expanding demand for service oriented applications increases the need for opening up these systems for interaction with external users and services. Opening up these systems for external users and services is not a trivial task. Thus, there is a need for a security layer which enables communication with internal applications and data while not compromising the integrity, confidentiality and availability of the system.

1.1 The solution

Cybercom Enhanced Security Platform, CESP, is an integrated platform that provides comprehensive security functions for high assurance applications that require high level of security and protection.

CESP has all the necessary components that together form a unique security platform for services and information. The platform provides the following functionality:

- **Authentication** - Assures that only trusted users can get access to the system
- **Access Control** - Make sure that authorized users only can access data he/she has the right to see. Also controls the ability to update data
- **Logging** - Collects information about all user activity in the system
- **Control and Audit** - Functions that can be used to control and monitor user activity in real time and to analyze logs and to perform audits.
- **Secure Communication** - Secure system for communications across network boundaries
- **Server Management** - Manages all services on all servers
- **Notification** - Notify senders and receivers in predefined situations in a secure and reliable way

CESP is based on the latest technology in order to create a robust and flexible platform that confirms to the highest standards of security and performance. For example, CESP meets the very high standards required by the Swedish public emergency and rescue enterprise SOS Alarm.

1.2 Result

The result is a platform that gives the customer the possibility to offer their external customers the following services:

- Access to internal services
- Access to internal data such as resource utilization and statistical summaries in real-time

CESP also provides a flexible and easily maintainable system where:

- Internal and external users and their access rights is managed in the same tool
- Different users can use different authentication mechanisms (e.g. username/password, smart cards etc.) based on the security requirements
- Attribute Based Access Control is used which simplifies the management of users access rights
- New users and authentication methods can be added very easily

This is all done while preserving a high level of security of the system.

2 Background

There is a large number of systems where the confidentiality, integrity and availability of the applications and all the data are of great importance. These systems can for example be banking services, health care companies, and governmental organizations which handle large amount of sensitive data. Typically, assuring the confidentiality, integrity and availability of these systems is done by implementing the system within a closed network environment where external users get no or very limited access to the applications and data.

However, the expanding demand for service oriented applications increases the need for bidirectional communication with these systems. There is a need for opening up these systems and to offer services to external users (e.g. customers). Besides the need for secure interaction with the system there is a need for a new solution to enable for further development of additional services.

Opening up these systems for external users and services, while preserving the same level of security, is not a trivial task. Thus, there is a need for a security platform which enables communication with internal applications while not compromising the integrity, confidentiality and availability of the system. The security layer should assure the identity of external users and applications communicating with the system without risking the integrity, confidentiality and availability of the internal applications and data.

One important aspect of a secure platform is the administration of users and their access rights. In order for these systems to be effective and useable, administration of users, both internal and external, and their access rights must be flexible and easy.

3 Overall Requirements

High assurance systems often require high performance and a high security level. On top of security and performance, special attention has to be focused on the following areas:

- Scalability
- Flexibility
- Monitoring and Logging
- Interoperability

The following section gives an overview of these development requirements.

3.1 Security

The following overall security requirements form the base for the CESP services.

3.1.1 Availability

The services should be implemented using effective and robust techniques and frameworks in order to get a high level of availability. Any problem with internal services should automatically be detected and handled by the system. If a problem is detected, the service should be restarted automatically without manual intervention. Calls to the systems which cannot be fully executed should be rolled-back and re-executed.

3.1.2 Confidentiality

The platform should ensure confidentiality i.e. ensuring that information is accessible only to authorized users while anonymous users should not have access to any service unless it is explicitly permitted.

Also, all communication should be secured against unauthorized access. It should not be possible to gain access to any information neither by external users listening on the network traffic nor by listening on the internal traffic.

Further, services should only be accessible for authorized users as long as they are connected to the network where the services are installed. External users should not get access to the publicly available services over an internet connection.

3.1.3 Data Integrity

The platform should assure that all data is consistent and correct. Information should be protected from being manipulated by unauthorized users, both during transportation and during storage.

3.1.4 Non-repudiation

The platform should enable the possibility to follow up and audit all activities in the system in order to assure non-repudiation. It should also be possible to trace and connect all activities to a user of the system.

3.2 Performance

The platform should be based on modern programming tools and techniques in order to assure outstanding performances for all services.

3.3 Scalability

The platform should have a scalable architecture that can handle the increasing demand for performance. Further, the architecture should be scalable in terms of adding new servers in order to meet up to future and higher demands of capacity.

3.4 Flexibility

Flexibility is one of the most important demands on the platform. It must be very easy to adapt the platform to adhere to new needs and requirements such as

- Adding new services
- Creating new data flows
- Automatic restart of the system without manual intervention
- Adding new authentication methods

3.5 Monitoring and Logging

The platform should log and monitor all events. This is important in order to detect any misuse or any unwanted behavior in the system. System and error events should be transmitted to the Windows Event Log to make it possible for MOM/SCOM to be used to collect logs from different system into one system monitoring tool.

Information about authentication, access control, configuration of services and access rules should be collected in a separate log to make it possible to assure the integrity of this sensitive information.

3.6 Interoperability

In order to enable a service oriented system, the platform has to be designed to interact with other systems and platforms. This is especially important for parts of the system that should interact with external users.

The service has to have a web interface that is compatible with the two major web browsers on the market, Internet Explorer and Mozilla Firefox. The publicly available web services should be available for both .NET and Java clients.

4 Platform Overview

Cybercom Enhanced Security Platform has been developed based on the latest technology to be able to create a robust and flexible solution that conforms to the highest standard of performance and security.

CESP consists of seven functional components that together form a unique security layer for services and data (see table below and Figure 1).

Functionality	CESP component	Description
Authentication	CESP-ID	Assures that only trusted users can get access to the system
Access Control	CESP-Access	Make sure that authorized users only can access data he/she is permitted to see. Also controls the ability to update data
Logging service	CESP-Log	Collects information about all user activity in the system
Control and Audit	CESP-Analyzer	Functions that can be used to control and monitor user activity in real time and to analyze logs and to perform audits
Secure Communication	CESP-Link	Secure system for communications across network boundaries
Server Management	CESP-Admin	Manages all services on all servers
Notification service	CESP-Notify	Notify senders and receivers in predefined situations in a secure and reliable way

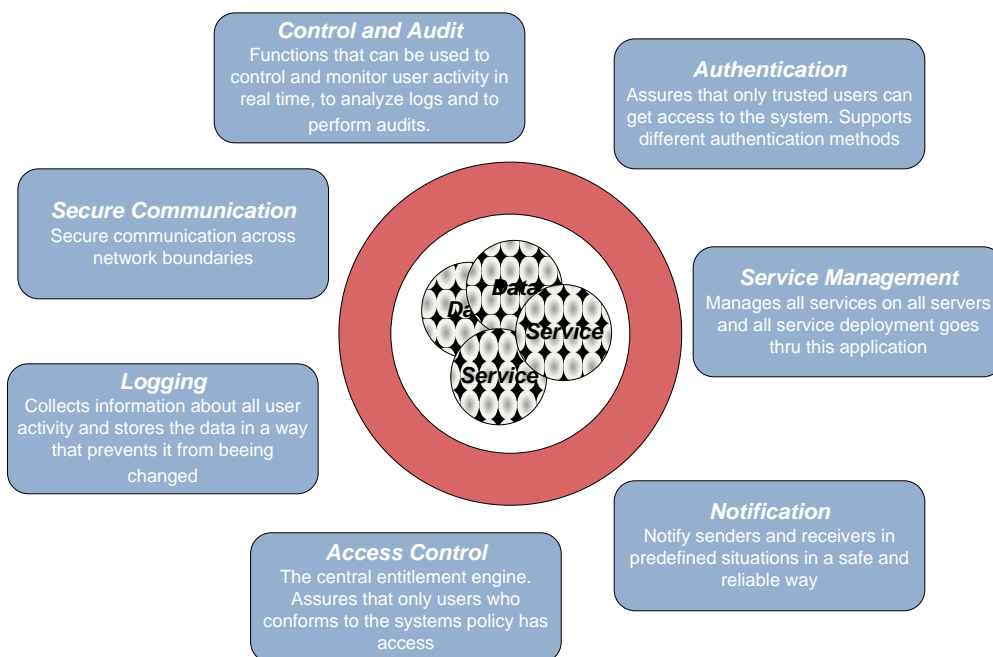


Figure 1. Functional overview of CESP

The following picture gives a view of the security platform:

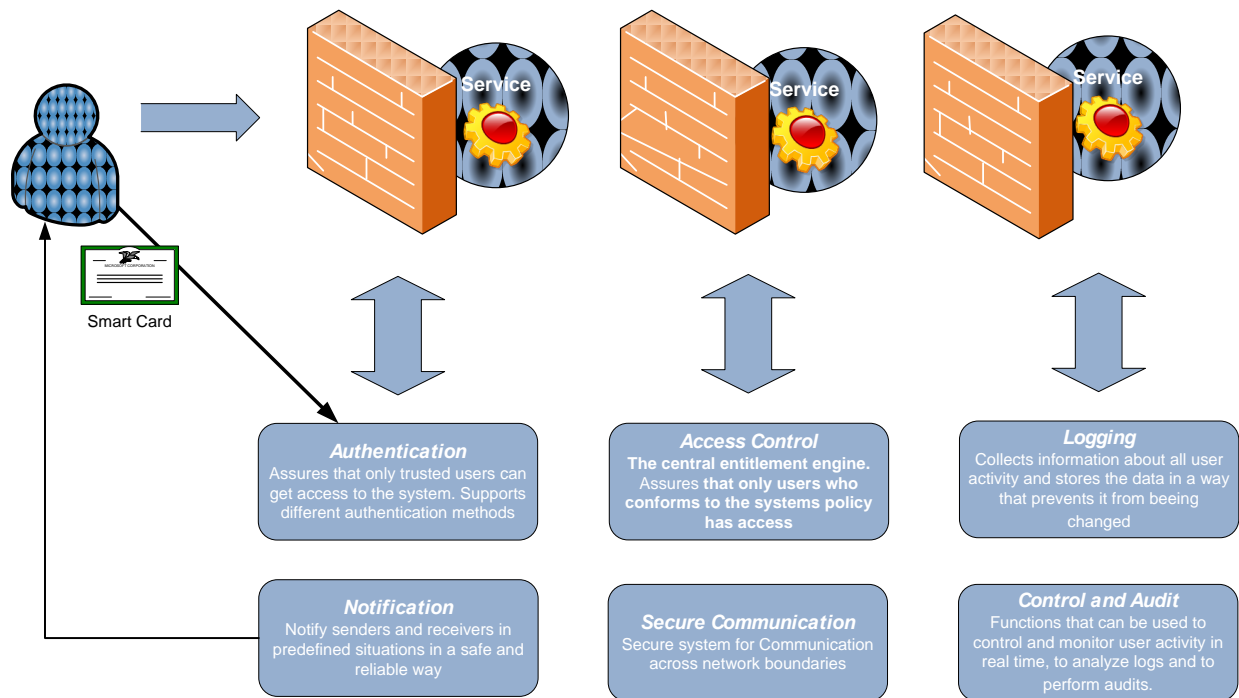


Figure 2. Detailed view of the security platform

By integrating CESP with a system implemented in a previously closed network environment, the system and its services can be opened up in order to provide secure access to specific services and data.

5 Technical Description

This chapter describes the technical details of the seven components in the Cybercom Enhanced Security Platform.

5.1 Authentication using CESP-ID

Authentication is needed in order to assure that only trusted users can get access to the system. In CESP, authentication of user is done using CESP-ID which is a flexible authentication solution that provides secure authentication of users and enables Single Sign-On between applications and organizations.

CESP-ID can handle different kind of actors such as physical persons or services. An actor can be authenticated using different methods by using Authentication Providers. Attributes can be retrieved from separate Attribute Providers. CESP-ID assures that an actor has been identified, authenticated, and assigned different attributes. This assertion is a signed proof and it can be used to gain access to an application instead of requesting a new authentication from the actor. In CESP-ID this assertion is based on the SAML standard.

The benefits of using CESP-ID is a more secure authentication and effective administration of user accounts at one place for all applications, and the possibility to provide Single Sign-On for enhanced user experience.

5.1.1 CESP-ID in detail

CESP-ID is a SAML v2.0 IDP that authenticates a user and creates logical tickets that can be seen as proofs of the authentication. It is possible to use different dynamic attributes depending on the way that the user has been identified. This creates a dynamic platform that is a solid base for further development. One example of this flexibility is that an identifier that is associated with a partner can be saved as an attribute in the logical tool which in a later stage then can be used to control which type of files that the user is allowed to sign.

CESP-ID is based on the Security Assertion Markup Language (SAML) 2.0, which is an XML-based standard for exchanging authentication data between security domains. CESP-ID supports several different authentication mechanisms and can be integrated with Trusted Security Server for providing verification of electronic ID (EID). CESP-ID is also compliant with the Swedish healthcare standard “Bastjänster för Informationsförsörjning“, BIF and also conforms to SAML V2.0 IdP LITE pro.

5.1.2 Services

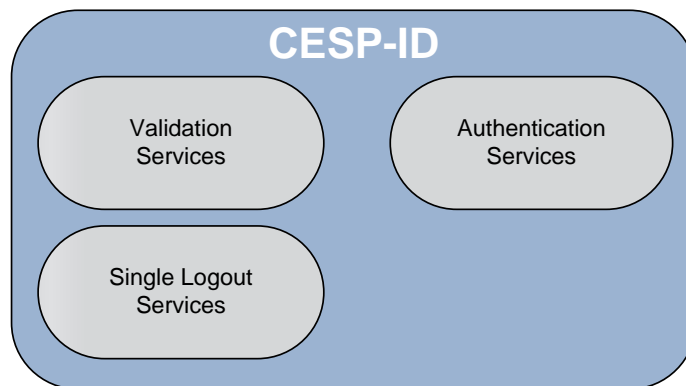


Figure 3. CESP-ID services

CESP-ID is built up by three services, CESP-ID Authentication Service, CESP-ID Validation Service and CESP-ID Single Logout Service, which together forms a flexible authentication

solution. It is possible to add new custom authentication providers as well as integration modules according to your organization's needs, thanks to CESP-ID's extensible design and use of web services interface.

The Authentication service can

- Verify the identity of the actor
- Assign attribute to the actor
- Verify the identity of an actor and it's attributes if requested by a service

By using a standard function for the authentication of users it is very easy to integrate access to other applications using the Single Sign-On functions in CESP-ID.

5.2 Access Control using CESP-Access

Access control ensures that an authorized user only can access data or a service that he/she has the right to see and use. Access control in CESP is performed by CESP-Access.

CESP-Access uses a technique called Attribute Based Access Control (ABAC). The application can, based on the users attributes, grant access to the information based on its own access policies. This way of granting access give much more flexibility than traditional access control based on groups or roles. It also reduce the burden of an extensive administration of groups and roles when a lot of different applications can be accessed using the CESP-ID Single Sign-On functionality.

The rules that govern the access policies are managed using a graphical user interface that makes it very easy and intuitive to define and test different access control rules.

5.2.1 Authorization Process using Axiomatic Policy Server (APS)

This section gives an overview of the authorization process. Once the user has been uniquely identified his/her ability to access data or application is checked by an authorization engine. CESP uses Axiomatic Policy Server as the authorization engine.

The authorization process (see Figure 4) is performed in the same way across the whole platform. The service call delivers a SAML ticket which contains the caller's attribute. This ticket has typically been produced by CESP-ID. All calls to a service always pass a check point that helps the service to determine if a request for an activity should be performed or if the call should be rejected. This function is called Policy Enforcement Point (PEP).

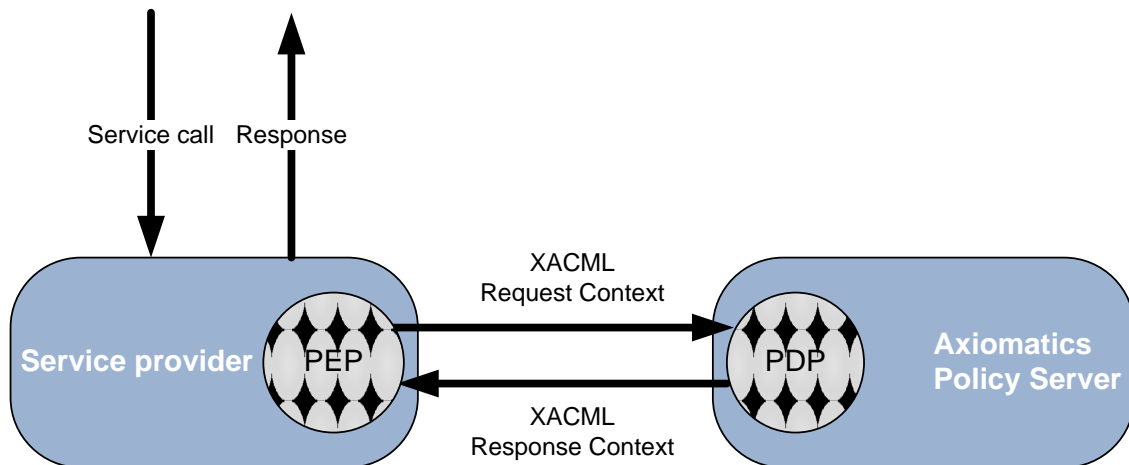


Figure 4. Access Control using CESP-Access

The task of the PEP is to collect properties of the caller, the attribute of the requested resources and other facts about the context in which the call is done. All this information is packed and sent to the Access Control that takes a decision if the call should be accepted or rejected. The right to get access to the resources is based on the attributes of the requestor and the attributes of the resource that is requested. This function is called Policy Decision Point (PDP) and is located in the access control service. The information is sent as a XACML Request Context.

All policies and rules are stored in the access control service and based on this, including the information from the PEP, an access decision is taken. The decision is sent back to the PEP in a XACML Response Context. The service can then get the decision from the PEP and reject or grant the user access to the requested resources depending on the answer.

5.3 Logging using CESP-Log

Logging is a central activity in a secure application in order to detect unwanted behavior in the system. CESP-Log is the central logging service that is responsible for the logging in CESP.

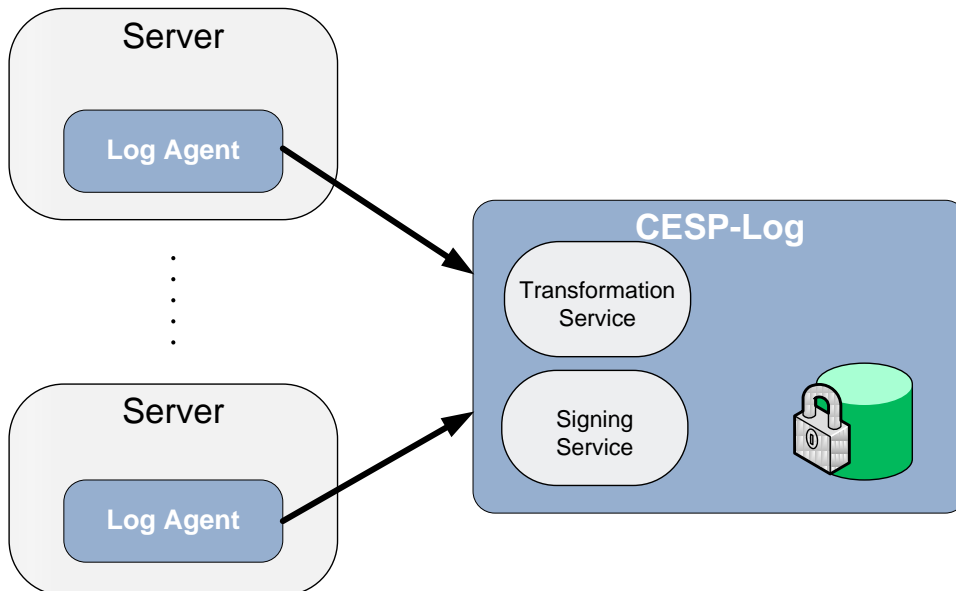


Figure 5. Log agents sends to CESP-Log

CESP-Log consists of the following components:

- The *CentralLogService* stores all log records in a secure database.
- The *CESP-Log LogClient* is used by applications to log information about events that occur within the application.
- The *CESP-Log LogAgent* is a service that runs on each system and gathers all logs from different applications on a system and sends them in batches to the *CESP-Log CentralLogService*.

All components in the security platform are configured to send log records to CESP-Log. CESP-Log collects log information using the log agents that are located close to the system that generates the log information. Logs are collected from all different levels in the system, from operating system, network components, database systems and application components. All log information is encrypted and signed and sent to a central log service where it is saved in a protected repository using signed log chains.

The local log agent can receive logs even if the central log service is not active or if the communication to the central service is down. The log agent handles this kind of situation by buffering the information locally. The log agent transmits this buffered data when the communication with the central server has been resumed.

The log service receives time stamped and digitally signed logs containing security related events from different systems like business systems, other CESP components etc. The Log service can handle different types of logs, where different logs have a well-defined content. For each type of log, mandatory and optional content can be specified in a XML-schema.

5.4 Control and Audit using CESP-Analyzer

For security reasons, it is important to be able to control and audit all the activities in the system. CESP-Analyzer is the component in CESP that enables this. The component CESP-Analyzer continuously analyzes the information that is collected by CESP-Log. This analysis can be performed in real-time to be able to send alerts when unwanted behavior has been detected. CESP-Analyzer can also be used to create scheduled reports for audit purposes.

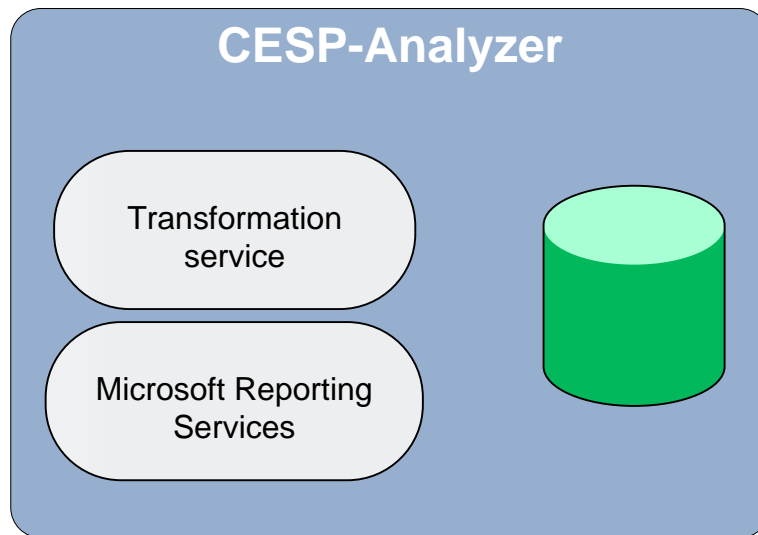


Figure 6. CESP-Analyzer

The benefit of having a central storage of log records from all systems within a domain is that it enables a more complete log analysis. CESP-Analyzer analyses all logs that have been collected by CESP-Log. Based on this analysis alert can be generated and sent out according to pre-configured rules. It is also possible to create graphical reports to visualize the logs and to be able to study different activities in detail. An administrator can create such reports using an intuitive graphical interface. Report creation can be scheduled so that standard reports can be sent out on a regular basis to predefined recipients.

Access to log data is controlled by CESP-Access. Access can be granted on different levels. CESP-Access can grant access to view log data and to create, modify and execute log analysis sets.

5.4.1 Analysis Process

The analysis of logs is performed in two steps. In the first step, the log files that has been collected by CESP-Log are normalized and predefined information from the log files are extracted. The next step is the analysis of the data using the report generator.

5.4.2 Reporting

Reports can be produced by CESP-Analyzer. It is possible to find specific information in the logs based on users, actions, time stamps, system or resources. Advanced searches can be performed in order to produce necessary reports.

By default the report contains the following columns:

- Time
- User
- Action
- System
- Resource
- System specific log message

Once a report has been created, it is possible to generate different output formats. The following formats are currently supported:

- On Screen report
- XML file with report data
- CSV (comma delimited)
- Acrobat PDF file
- MHTML (web archive)
- Excel file
- TIFF file
- Word

5.5 Secure Communication with CESP-Link

It is necessary to be able to set up secure communication between different network segments within the system in order to exchange data and to access services. This has to be done with a minimal effect on the protection borders between the different networks. CESP-Link is a solution for the management of work flows and applications across different server and across network borders.

CESP-Link has a system to control incoming calls where origin and service document is applied on the service register and settings that is distributed using CESP-Admin. The result is that individual service components are executed and that the answer is returned directly or that the workflow scheduler is used to schedule the activities. On each server, CESP-Link is running as a Windows service which makes it possible to connect different components that forms a service.

The following picture shows the basic architecture for CESP-Link. It describes how the different components are distributed across the different network segments.

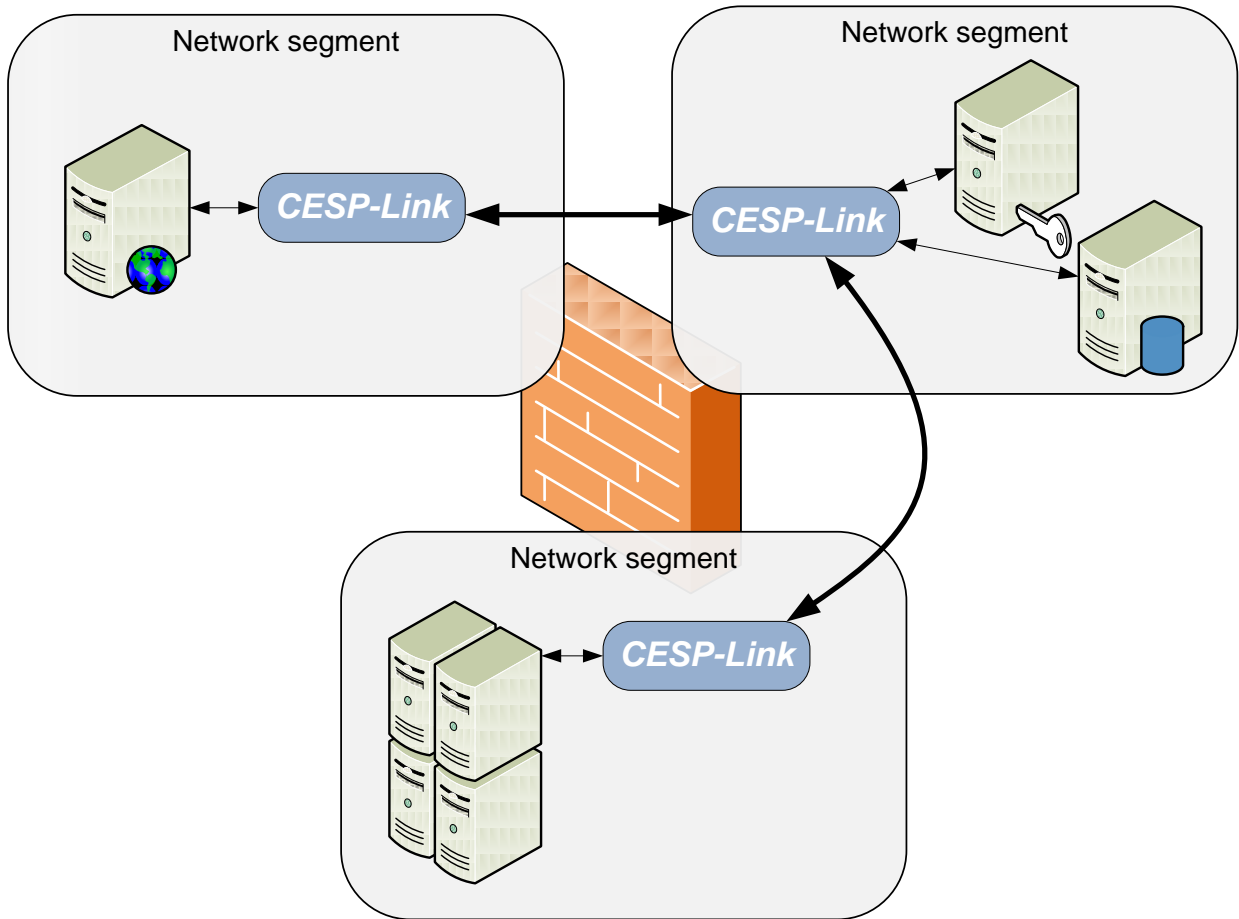


Figure 7. SureLink

CESP-Link enables transparent communication between components in an application, i.e. components can communicate with each other without knowing the others location. In the same way it is possible to access the work flow engine from each component across the whole network.

5.6 Server Management with CESP-Admin

CESP-Admin is a separate management module in CESP which is used for managing components and services on all servers in the environment. It is also used to get status of the different servers and to produce diagnostics. The service is available via a web application that communicates with a Windows service on every server in the platform.

CESP-Admin has the following basic functionality:

- Manage servers
- Add and remove services as service components
- Add and update work flows
- Update settings for basic services
- Produce status reports and diagnostics

The figure below shows an overview of the functionality of CESP-Admin and its connection to other entities in the platform:

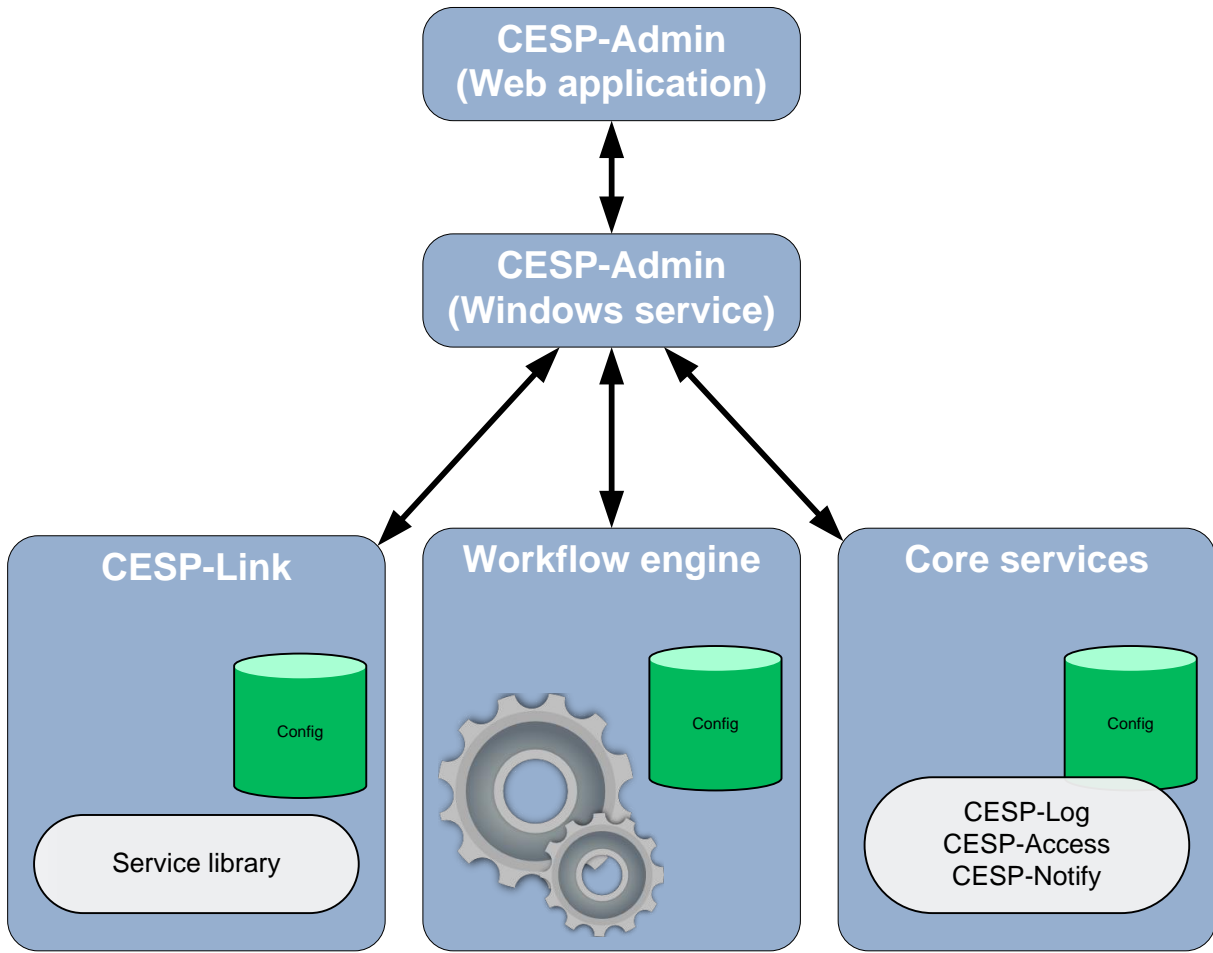


Figure 8. CESP-Admin and its connection to other entities in the platform

CESP-Admin also provides a flexible portal solution which enables configuration of user-specific portals based on the user's need and authority. The Admin Portal can also contain calls to other services that are needed for the management of the solution e.g. PKI-services.

5.7 Notification by CESP-Notify

CESP-Notify is the Notification service that enables transparent notifications to senders and receivers. CESP-Notify assures that notification is performed in a way that handles:

- Security
- Signing of the message
- Guaranteed delivery
- Secure/unsecure delivery
- Receipt
- Message ordering

CESP-Notify uses the publish/subscribe message paradigm which enables the possibility for a sender (publisher) to notify one or more recipients (subscribers) without the need for the sender to know the receiver or in which way the recipient is notified.

CESP-Access controls who can send and receive messages using CESP-Notify. CESP-Access also controls who have access to the management interface.

5.7.1 Notification procedure

CESP-Notify is based on the standard *WS-Notification* and uses *BrokeredNotification* with the method “*Simple Publishing*”. Using this method, the publisher sends a notification message to CESP-Notify, when a certain situation occurs that the publisher wants to inform about. CESP-Notify will then send a notification message to all subscribers which have been registered to receive notifications about this specific event.

The notification message can be sent in many different ways and each subscriber specifies at registration time in which way they would like to be notified. When the subscriber receives a notification, it sends a confirmation message back to CESP-Notify. CESP-Notify in turn, inform the publisher that the message has reached its subscribers. If the message on the other hand doesn't reaches its subscribers within the specified time frame, the publisher will be notified by CESP-Notify. In such a case it is up to the publisher to decide which actions that is appropriate.

5.7.2 CESP-Notify components

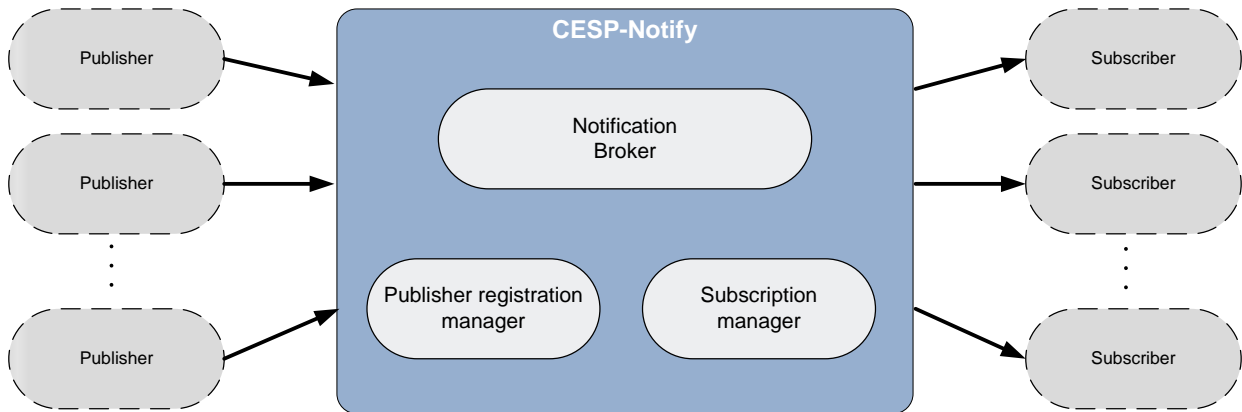


Figure 9. Notification process with CESP-Notify

CESP-Notify consist of the following components:

- The *PublisherRegistrationManager* is responsible for receiving registration requests from publishers. This service can be configured in the way that the publishers have to register before they can send notifications. At registration time the publishers can be authenticated.
- *SubscriptionManager* is responsible for registering subscribers for the different notification types and how they would like to be notified. To register a subscriber, the *SubscriptionManager* is either called by a specific recipient or by users with the authority to register recipients for a specific notification type.
- *NotificationBroker* is responsible for accepting notification messages and sending them to the registered subscribers. A subscription describes the connection between a subscriber and a notification type and describes how the subscriber would like to be notified.

6 Conclusion

This paper describes Cybercom Enhanced Security Platform. It serves as a security layer for systems that needs to be opened up for external users and services where the confidentiality, integrity and availability of the internal applications and data are of great importance.

CESP is built using the latest technology in order to achieve high performance while preserving a high level of security. The architecture is scalable and flexible in order to meet future needs of performance and new security requirements. The resulting platform enables a secure service oriented system.

CESP can be integrated with already existing systems which enables a cost-efficient solution that enables efficient and effective interaction without compromising the integrity and confidentiality of the system.