Concept *Trusted Access Paths* Belastingdienst

Research Report for Research Project 2 - version 1.05
Master System and Network Engineering

University of Amsterdam

Fangbin Liu
student number 0291536

Steffen van Loon
student number 0611360

July 4, 2006

Abstract

This document describes the TAP-concept and our research towards it. This project is part of our study "System and Network Engineering" at the University of Amsterdam. The project is done on behalf of the *Belastingdienst*, the Dutch Tax and Customs Administration, further referenced in this document as the TCA. Our research exists of a literary study of the TAP-concept based on documentation of the TCA and other sources, and the description of an existing small environment as TAP-concept as proof of concept.

The TAP-concept is a model in which trust relations are described in process chains, consisting of the security functions authentication, authorization and verification. The implementation of this model in these aspects will be investigated and discussed. At the end of this project, an evaluation of the applicability of this new concept will be given.

Contents

1 Purpose and motivation

This document was written as end deliverable for our second research project, which is part of the course System and Network Engineering at the University of Amsterdam.

This project is done on behalf of, and under supervision of the *Belastingdienst*. The *Belastingdienst* is the Dutch Tax and Customs Administration, and is further referenced in this document as the TCA. Our supervisor from the TCA during this project is Norien Kuiper, and our University supervisor is Cees de Laat.

The purpose of this project is to study and evaluate a new security concept developed at the TCA. This concept is called *"Vertrouwd ToegangsPad"* (VTP) and describes a secure access concept on the basis of defining trust relations. This concept will be further called *Trusted Access Path*, in short *TAP*.

The project consist of a literature study of the documents provided from the TCA. After analyzing this concept, we will try to use this concept to describe a technical environment where the TAP concept can be applied.

The authors want to thank Norien Kuiper for her contribution, support and feedback during this research project. We also like to thank Ernst Mellink and Hugo Heitmeijer for their input and explanation of the TAP concept during an interview with them in Apeldoorn.

The main question that will be strived to answer in this project can be stated as: whether the new concept called TAP is realizable in a small environment (and eventually within the TCA). The research will focus on the application of this concept with the standard techniques that are available on the market at this moment. Various aspects of this concept will be investigated and the main reasons of development will be analyzed.

First, we will try to describe why the TAP-concept is developed, and from which developments this concept is requested and generated. Next, the concept will be introduced and analyzed where the various aspects of the concept are described such as registration, authentication, authorization and logging. On the basis of the description of this concept, the applicability with this concept will further be discussed. After introducing this concept, we will focus on the analysis of a couple of systems where the TAP concept can be realized. Within these systems, the trust relations implemented among components in the system will be discussed.

At the end we will describe our research conclusions and try to make some suggestions for further development or attribution. As conclusion of this project, we will give an evaluation of the practical value of the TAP-concept and also the outlook for the future development trend for this topic. The legal notes are attached in Appendix A - Creative Commons Licence.

2 Why TAP?

This section describes the reasons why the TAP-concept is introduced. This will consist of the following descriptions:

1. development within TCA (customer-pull)
2. development on the market (market-push)
3. impact and conclusion

2.1 Development within TCA

In 1 it can be seen that the security protection within the TCA is organized in a "onion" form. The most outer circle stands for the physical security. This means all the entrance to the environment where the computers networks of TCA sits will be secured through various techniques such as smart card. It is supposed that in this way, only the person authenticated by the TCA will be allowed to access the machines. Next, the middle circle in the model stands for the logical closed technical infrastructure. With this layer of protection, the user must supply the identity to the system before it can enter the system to access the data within it. This forms a gate between the internal system and the user which let the user be authenticated by the third circle. The third circle stands for the logical data access control which will carry out the work of authenticating the user and give the user the access rights to the internal data.

On multiple occasions the conclusion was made that the current policy based on the "onion"-model does not suffice any more. There are some administrative gaps in the organization of the security concept based on the current layered structure. Also some technical issues apply, for example connections to other networks should only be allowed in a controlled environment. The conclusion after some research and experiences was that the control on these connections is impracticable, due to insufficient supervision.

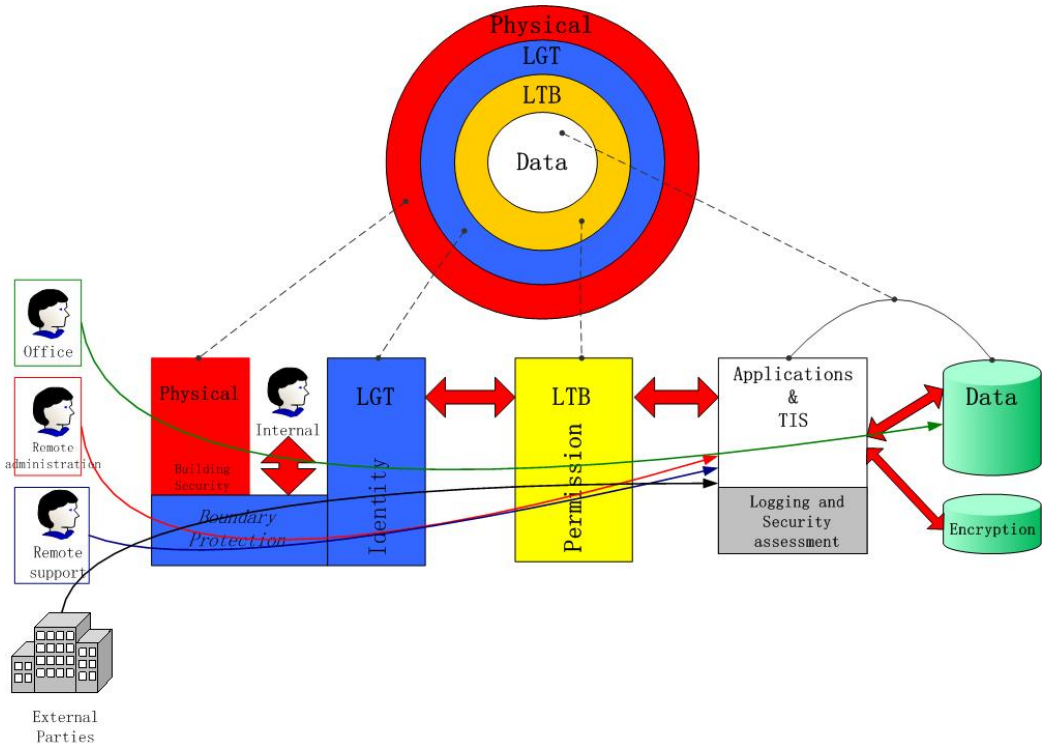


Figure 1: Onion-model

Internal as well as external auditors are pointing to facts which indicate that the current infrastructure is not conform to the minimal security requirements.

Especially, the conditions that are required for the traditional concept are not met anymore:

- not all hardware, software, data and users are known and trusted
- the access to data is not fully applied through authorized applications with trusted users
- the transmission of data to external parties is not always done through controlled ports with authorized applications
- the complete ICT architecture is not fully covered with a physical security layer

Besides these organizational problems, there are two key questions regarding responsibility:

- placement of risk management: there is no explicit part of the organization dealing with risk management involving the use of ICT.
- the responsibility of information, authorizations and processes is not clear due to changes in the organization.

2.2 Developments in the market

The life-span of the current policy based on the onion-model is expired from a technological point of view. The onion-model is based on the fact that all computers and networks work in a known stable configuration, on which only authorized employees can make alterations. Also the assumption is made that the traffic on the network is only viewable by authorized personnel. Both these assumptions are not valid:

- office networks nowadays have an open structure, and there is no structural control to prevent unauthorized changes.
- traffic on these networks can easily be tapped, from which passwords can be captured.

The current developments are all pointing to a more global provision of service. This means that a lot of the activities and operations are not only

provided within the buildings of the TCA anymore, but also on other locations. Future services will probably also be provided via other communication channels like the Internet. When these services are not provided within the current protected environment, the current assumptions on the security are not met anymore.

Various techniques are developed on the market to strive to supply more security functions for the various new services on the internet. This market trend can be viewed in various aspects. As stated in the document [5], firstly, the risks existing for the new generation of internet services are realized and monitored more intensively nowadays. This result comes from various attacking possibilities on the internet, such as hacking, viruses and users' operational fault. To protect the system connected to the internet against all these kind of risks, various technologies have been utilized. For example, the EDP auditing organizations have put more attentions on virus scanning. Also, various anti-virus application systems are developed.

Secondly, security has been divided into various aspects so that more advanced divisions of the techniques for various aspects of security can be made and the techniques can be more intentionally utilized. Under the security infrastructure, four main aspects are generated. These are identity infrastructure, permission infrastructure, encryption infrastructure and logging infrastructure. Various products have been introduced into the market for these purposes. Some special security system products for Boundary Protection and Intrusion Detection are produced also. Also, at the organizational level, the focus has been switched onto the standardization of the system, which means that more security should be achieved from the infrastructure instead of the application or process before.

Last, the security has been viewed more and more as a standard conditions for the service to be supplied on the public market. All the internet services nowadays must be able to supply a good security system for the users so that the integrity and the confidentiality of the services can be guaranteed.

2.3 Impact and Conclusion

The previous section describes some reasons why the current environment is not fully secure. All the problems mentioned, the changing infrastructure with increasing components and users, and the changing set of demands such as increased connectivity all lead to one conclusion: a new security concept is indispensable.

3 The TAP-concept

To solve the problems described in the previous sections, a new concept is developed and proposed to be implemented in new applications and infrastructure. The reason why the TAP concept is introduced will be supplied first in this chapter. After that, the definition of TAP will be given. At the end of this chapter, a global description of the possible areas where TAP can be applied will be given. It can be seen as an introduction for the more concrete description in the next chapter.

3.1 Origin and description of TAP

The main reason for the introduction of the TAP-concept is to provide an additional model for development and exploitation within the TCA, from which the security requirements needed for the TCA are achieved again. This model should adapt to the strategic decisions which apply the development line. These demands are as follows:

- all obscurities regarding functions and responsibilities are cleared. The new model should give the owners of processes, data and authorizations the means to clarify which risks are taken, and which risks are intervened
- all dependencies on the physical security are combined and minimized
- data access is only possible through authorized processes

Key functions in a secure infrastructure are identification, authentication, authorization and verification.

Identification and authentication of a user or process ensures that we are dealing with that particular user or process. Authorization assures that the particular user or process only performs actions that he is explicitly allowed to. Verification assures that there is a form of control that enables to verify all steps after the performed actions. The problem is that without a good model these functions are implemented several times. This results in a situation that is ineffective and inefficient. Users and administrators have to do more actions (for example: multiple logins), and the implementations of these functions differ in strength, which results in a less secure environment.

The definition of trust relationships could be a solution for this problem. These trust relations can be defined as a surmise about the behavior of an

other party. The surmising could be for example that another party correctly arranges the authentication of a user. Another example of a trust relation is a client-server application, in which the clients assumes that the server functions correctly and vice versa.

The term trust relationship is usable in many situations where parties communicate, but the assumptions about each others behavior are not always explicitly mentioned. In these situations some assumptions are made implicitly, and thus do not describe the correct functioning. With the *Trusted Access Paths*-concept, all assumptions are described explicitly and only at the points where trust is of interest in the security of information systems. This means that only the previous mentioned functions are described: identification, authentication, authorization and verification.

In this TAP-concept there are some decisions on these functions which are foundations for further describing trust relations:

- registration of users is done by one process (as much as possible)
- authentication of users is done by one process
- there is always a mutual authentication between processes in a process chain.
- authorizations are granted to users and not to processes
- the complete access chain between the user and the protected object is verified (logged)

These choices are translated to modelling decisions for each of these functions. If this complete model is used, then it will be possible to accommodate the implementation of the security functions in a generic infrastructure for authentication, authorization and logging. Then this infrastructure can be invoked by applications, which eventually will lead to simpler applications, because these security functions are not accommodated within each application anymore. This single implementation of each function in a generic system can be better and stronger, which will lead to a more secure and simpler environment.

The implementation of this concept will definitely have impact on developing applications and components, so the TAP-concept can be a reference point for defining new API's and interfaces. This is however not part of the scope of this document and research.

The goal of the TAP-concept is to define an environment with single implemented security functions. Defining and describing mutual trust relationships

helps to make clear which considerations were made when making choices in the implementation of the infrastructure. This makes clear where all functions are implemented, and what security level they achieve. The integration of these security aspects in strategic and tactical development processes helps with the explicit description of risk management. Primary achievements can be as follows:

- reduction of complexity
- reduction of administration
- better control
- better reporting

What is TAP

A good example for the utilization of the TAP conception can be found in the next model.

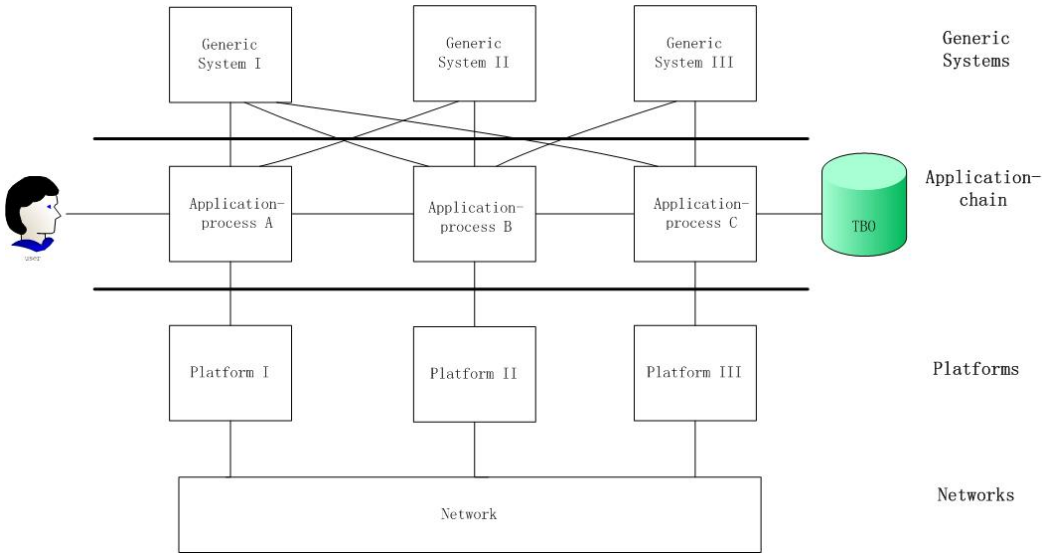


Figure 2: A figure of TAP for the data access process chain

As shown in 2, a data access path is formed by a chain of alternative processes from a user to a database. With the concept of TAP, the most important issues of the security control for this path can be overviewed and managed in a very efficient and effective manner. The security for this path requires

that it should be impossible for users outside this path to gain access to the protected object. Also, it needs to be ensured that the users outside this path can not break into this path through some other ways. To make these requirements to be fulfilled, a number of security approaches can be implemented for different application processes. These methods consist of user identification and authentication, rights authorization, events logging and data encryption. In this way the processes in the above process chain can be secured and together form a secure data access path from user to protected object.

The above model can also be seen from the perspective of trust relations among processes. Since an absolutely secured environment is impossible to achieve, secured processes must be used within a process chain. Through utilization of secured processes within the chain, a trust relation can be built up among processes. This means that every process can utilize another secured process in order to keep the security within the whole chain at a high level. A trust relation between processes means that a process can assume that the behavior of the other process is normal and that the correct results are returned. Through this kind of assumptions among the processes in a chain, a trust chain can be formed. In this way, the security within the whole chain can be overviewed and managed easier.

To realize the trust relations within a process chain, security methods must be deployed. Since there are various trust relations at the different points of a process chain, also different methods need to be deployed respectively. Inside a process chain, the internal processes can be secured through utilization of special infrastructure, or special combination of security methods. It can be seen that this kind of security is easier to manage than the security by the edge of a process chain. This edge can be the point where the process within the chain communicates with the user outside the chain. Since the behavior of external users is impossible to define, the security control for these parties will be a heavy point for the whole system. In other words, the security of the whole process chain depends on the weakest point in the chain. And it is very possible that the point between internal processes and the external user would be at this point. As a result, more attention should be placed here.

To make a process chain trustworthy, various methods can be used inside and outside the chain. For a process within the chain, the behavior of the process can be defined and controlled by all the various mechanisms. For a process

on the edge of the process chain various security methods are available to make this process trustworthy. The users identification, authentication and authorization processes must be supplied. Furthermore the integrity of the codes used by the processes must be kept and controlled. Some special set of rules can be made for this purpose. The security methods mentioned above should be applied in the infrastructure level, instead of the application level. This means that the security methods must be overall applicable, not dependable on the applications where it is utilized. By this kind of settings in the system, the security within the system can be guaranteed efficiently.

3.2 Where is the TAP-concept applicable?

The concept of TAP can be utilized in various enterprise environments where a secure data access path is required. With the use of the TAP-concept, the data access can be secured and only granted on the authenticated user or process. The system where the TAP-concept is applied must fulfill a number of requirements so that the concept can be utilized efficiently and effectively. As stated in [5], these requirements include:

- The components within the system infrastructure should be loosely connected with the applications deployed within the system
- The different parts should be identified clearly so that their tasks and relations with other parts can be recognized simply
- The function should be realized with simple infrastructure or application structure
- The data being accessed and needed to be protected should be stored in a simple database infrastructure where the communication with the system applications is defined

Once the target system fulfills the requirements mentioned above, the TAP concept will generate many advantages while supplying multiple functions for the system. First of all, since the execution of the application does not depend on a specific server or device, the flexibility of the utilization of various applications in the system can be realized at a high level. It means that the application can be replaced with other applications easily and without changing the infrastructure.

With a clear structure of relations among the components within the system, the security issues within the system can be defined and controlled more

simply and efficiently. The management work of the system administrators can be reduced significantly. Furthermore with a clear data storage structure picture, the data access security can be controlled and defined clearly.

Through the utilization of a clear and simple system structure, the points where the security processes identification, authentication and authorization needs to be implemented in the infrastructure level, will be clear and easy to manage.

Together with the advantages generated by the utilization of the TAP concept, a number of difficulties have to be discovered. A direct result of the introduction of the TAP concept into applications can be the fact that many applications need to be changed or implemented again. This comes as a result of the fact that in the new TAP concept, the security functions are a generic service supplier, but not a application-specific function.

Since all the data access paths from the user to the data resource must be secured with the process chain mechanism, the security policy must be stated as completely as possible so that every point in the system can be secured. Since the user behavior is the hardest point to manage, the security of the whole system will depend on the security at this point. Therefore, extra policies and mechanisms will need to be stated for this security point.

To form a trusted path from users to data, the security among the internal applications will also need to be implemented through completely secured mechanism or functions. A good example for this kind of security can be the trust relations among various servers within the system. If the servers are all located in some certain secure environment in the TCA, then there will be less requests than the case where servers are located in a distributed environment. In the second case, the security mechanism will be necessary to verify the correctness of identities of the communication parties.

4 Application of TAP-concept

4.1 Business requirements

There are some requirements necessary on the process- or business structure for deployment of TAP. All development that the organisation should make is not part of this document. An important part which should be accounted for is that is should be clear who is the owner of the processes and

data. All granted authorities shoyld be clear, and authorized users should be trusted. All technical messures are supporting, the organisational meassures are decisive.

An other important point is that all users should have an identifiable devision of roles, like ITIL, and that each employee has a limited set of roles. The number of roles in the organisation should be limited.

4.2 Technical requirements

In this section, on the basis of the business requirements described in the previous section, the technical requirements on the system for the realization of the TAP concept will be discussed. Various ICT-components for the TAP-concept include the generic system infrastructure, the identity management infrastructure, permission management infrastructure, encryption infrastructure and logging infrastructure. The requirements on each components will be listed and the problems for the systems will be analyzed respectively. Among them, some principles of the system infrastructure will be stated such as single sign-on for Identification, role-based authorization, convertibility of identity from process to user for logging system and so on.

4.2.1 General Issues

To realize the TAP concept within the enterprise infrastructure, a number of ICT components must be utilized. These components should ensure that the security on the path from end users to the enterprise database can be guarded. Thus, to keep the whole path from being broken or misused, a number of components need to be implemented. These components ought to include at least: general security issues, identity management for the users, permission management for the task executions, encryption mechanism for the data transfer and logging infrastructure for security auditing purpose.

The generic security issues should include the security protections invoked among various sub-components within the entire enterprise network system. The data transfer among various domains within the enterprise network should be limited and controlled. Also, the data access rights for the users in various sub-domains should be controlled and limited with the filter functions or control mechanism at the edges among various domains. In this way,

the data access rights can be granted only to certified users but not on others.

Furthermore some generic services utilized publicly by the components within the whole enterprise network need to be implemented. For this kind of services, the server to server communication should be guaranteed and controlled on the connections among various servers.

4.2.2 Identity Management

For identity management, external users outside the TCA should be requested to supply their identity before they can access the internal services supplied. The identity supplied by the end user should be authenticated and utilized to acquire the rights granted. For an efficient permission management, a role can be used for each identity stored. For each kind of role, the permissions can be defined by the application being requested. There are various directory services available on the market. Well known examples include IBM Tivoli, Resource Access Control Facility and Sun One Identity Server. All these systems supports identity management based on role specification. Other systems that could be interesting for the TCA are *A-Select* and *Shibboleth*.

For various applications, the identity control should not be executed multiple times. Instead, a single sign-on mechanism should be implemented. It means that every application communicating with users must have a connection with a identity management component. The identity management component can be considered as a generic server supplier. To let other applications make a use of this component, the identity management component can be placed as a central accessible object.

A web portal can be used to realize such a single sign-on feature. The available applications for a particular registered user can be accessed via such a portal. The applications on the list will delegate the user credentials to finish the tasks required by the user, when other application are accessed. Through supplying the identity of the application and the end user, other applications can verify the applier and control the executer of the request via various mechanisms.

4.2.3 Permission Management

For the permission management, the central identity management function can be combined with permission management within the application environment. It means that rights granting decisions can be made based on the identity received from various applications. To enable the permission control among processes, various identity verification methods can be used within the communicating processes. Each process must be able to verify whether the request received comes from a permitted party. The possible identity verification methods include key exchange and connection parameters verification.

For the authentication between two applications, the certificates issued by a third party can be utilized by the SSL session between two communicating parties. Although in this way, some kind of attacks is still possible. Thus it should be guaranteed that the certificate supplied by processes must be able to be verified or used to decide whether the certificate of the other communicating party can be accepted or not.

The permission of the execution of certain tasks can be granted on the basis of the system environment. This means that the system will decide whether a user can utilize some applications based on the role associated with the identity of the user. The position where the data authorization control can be executed is at the starting point of a data access chain of processes and at the endpoint of such a chain. This means that only the processes at these two points need to communicate with a authorization module within the environment.

4.2.4 Encryption

Encryption management is not one of the basic components within the TAP concept. But since it is important for the data transfer in the TCA environment, it still needa to be implemented adequately. For various data transfer cases, different encryption methods can be used. SSL encryption methods are most utilized for network data transfer and is also proposed to be used within the TCA environment here. More complete description of the encryption methods being utilized can be found in the document [4].

4.2.5 Logging Management

The logging management should be able to supply enough execution records for each part of the system. With the help of these information, verification of the correct running of the system can be done. The places where the logging records are generated and gathered should be able to cover all the processes within the system. In this way, the security in the whole system network will be able to be guaranteed and audited later.

To save all the log records collected from various processes, a central log record could be used. In this way, the logs will be able to be audited later in a very efficient manner. Also this structure could make the correlation among various records more easily. Through verification of the order of certain events in certain systems, the security within the system can be verified and evaluated efficiently.

To collect the logs from various processes, a distributed log collector system can be used. In this way, the remote process execution log can be collected by the local agent. Next, it will sent them back to the central gathering point, where the logs are stored. The information that need to be logged can be divided into different levels, such as application level, network level and platform level. By filtering the logs on the basis of these levels, the behavior of some components can be reviewed more clearly and simply. Furthermore, the correlation among various levels will generate more meaningful data for the auditing purpose.

5 Application in Proof of Concepts

In the following sections we try to put the TAP-concept into practice on a small existing environment. The utilization of the concept applies to the functions identification, authorization and logging. With the description of the authentication function it is pointed out if the identity information is passed through and if this information is authenticated or not. This is indicated with the following acronyms between brackets:

I&A Identification and authentication are performed

I Only identification is done, the identity is passed without authentication by receiving party.

\- there is no identification and authentication

With the description of the authorization function the following indicators are used:

NAC No Authorization control

SA System authorization is used (privilege on system level, or using ACL)

AA Application Authorization (when available in the infrastructure, the generic authorization system is used here)

In the next sections we try to desribe the applicability of the TCA-concept in a small virtual environment as a proof of concept

5.1 MijnUvA Portal System

MijnUvA is a gateway website for the students of the University of Amsterdam (UvA). The students can use this portal to get access to personalized services supplied by the UvA, by logging in with their account registered at the UvA. On this portal page, the services that can be supplied to a particular user are listed. A student can choose which application he or she would like to use. Examples are access to web-based email or the Blackboard learning system. In the next sections we try to describe this system via the TAP-concept. This description is divided in a section for authentication, authorization and logging.

5.1.1 Authentication

As shown in the figure 3, the following trust relations for the Portal-system can be defined.

1. (a) The operating system does not validate the browser. (-)

   (b) The browser supposes that it communicates with a PC environment which has an authentication system that can be trusted (-) The browser asks for the user identity by the authentication system in the PC environment. (I)

2. (a) The web browser on the user machine verifies the identity of the web server (I&A).

   (b) The server application supposes that it communicates with a valid browser.

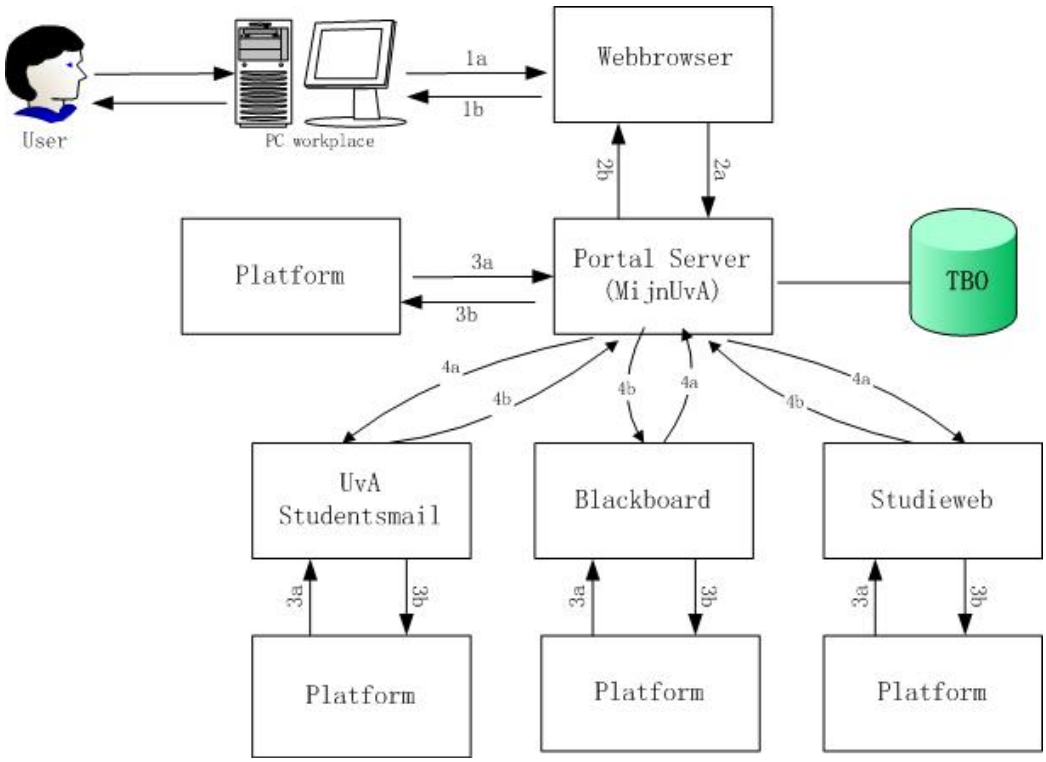


Figure 3: Trust-model for authentication with the use of a browser with MijnUvA Portal-system

The server application achieve the identity of the user from the browser (I).

3. (a) The platforms supposes that the particular server application is a valid process, the platforms does not verify the identity of the server application. (-)

   (b) The server suppose that it runs on a secure platform. The server does not validate the identity of the platform. (-)

5.1.2 Authorization

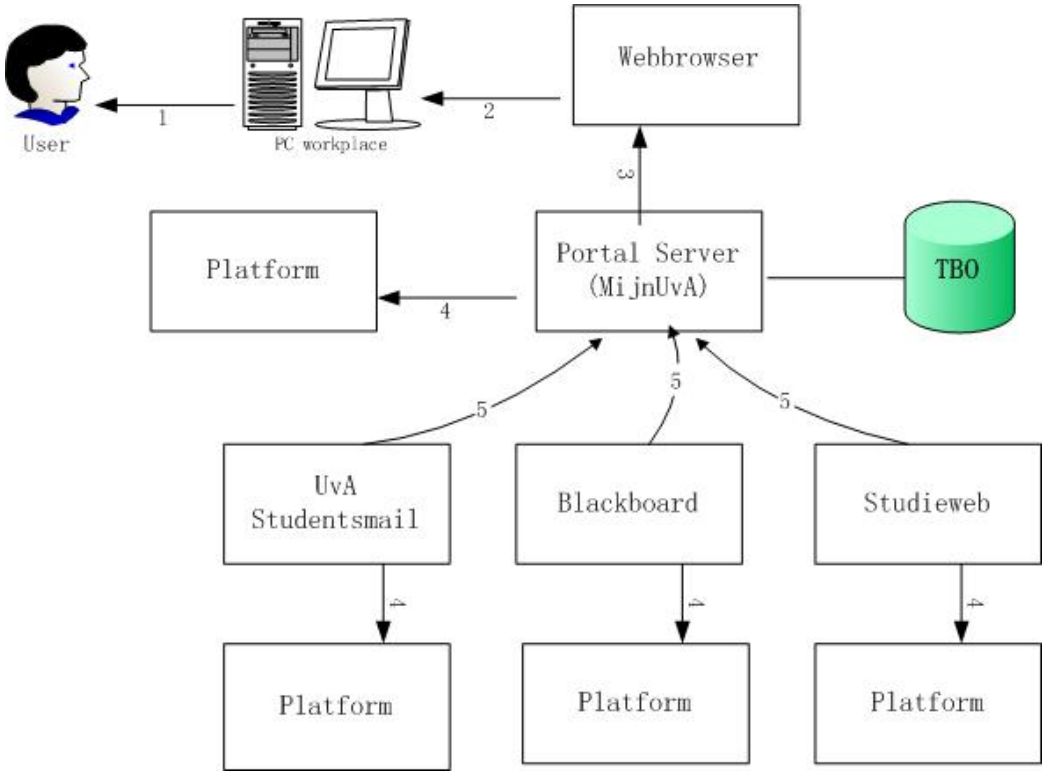


Figure 4: Trust-model for authorization with the use of a browser with MijnUvA Portal-system

As shown in the figure 4, the following trust relations for the MijnUvA Portal-system are be defined.

1. After a successful login, the user is granted with the right to use the machine (SA)

2. The PC environment has the authorization to start the web-browser (NAC). Each user has the right to use the web-browser, but due to the log-in procedure of the system authorization this is also managed. Each user that has the right to use the machine will automatically be granted with the right to use the browser on that machine (SA).
3. - The browser is authorized to communicate with the server application, but this is not explicitly verified (NAC).
   - The browser trusts that the server will handle the authorization control for the user (AA).
4. The server applications are allowed to run on the particular platforms (NAC).
5. The server applications can be used by the users after they are authorized by the Portal system (AA).

5.1.3 Logging

There is no trust-relation within the logging facility with the use of a web-browser as a client. As shown in the figure 5, the particular server applications will record all communication and transactions that are performed.

5.1.4 Conclusion

The previous example was pretty strait-forward and simple. This example looks a lot like the example in [6] describing the "Browser based passive client". Only difference is the single sing-on mechanism implemented in this example.

5.2 Eduroam

In the next sub-sections the main aspects of the Eduroam security environment will be analyzed. Through these analysis, it can be seen that TAP-concept is not so clear or easy to be applied in this environment. This is because the number of conditions used in the TAP-concept are different in the Eduroam environment than in the example configurations described in [6].

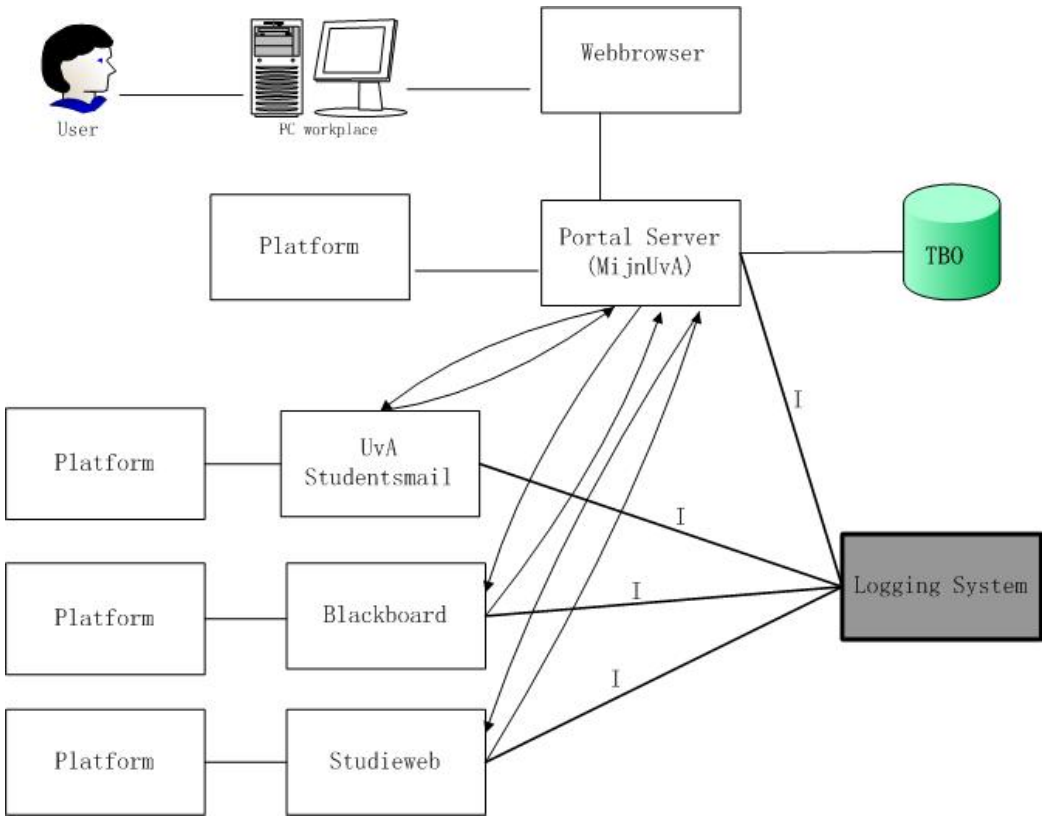


Figure 5: Trust-model for logging with the use of a browser with the MijnUvA Portal-system

5.2.1 Overview of Eduroam

Eduroam is a cooperation between Surfnet and educational institutes in which all parties share their authentication infrastructure for guest-usage of their (wireless) networks. This service is based on the 802.1X-standard, builds on a hierarchical system of RADIUS-servers, and supports web-based authentication. More information of this project can be found at the website of Surfnet [7][8] and Eduroam [9][10].

This service requires the installation of a X-supplicant on the client. This supplicant transfers the user credentials, via the switch or access point, to the RADIUS-server of the local institute. This server will lookup the user name in de local user-repository. If the user has a different realm (for example: the local realm is *@university-1.nl*, but the user has *pietje@university-2.org* as username), then de authentication and authorization request is transferred to the General Proxy RADIUS, and forwarded to the RADIUS server belonging to that particular realm. The acknowledge of a successful authentication travels back over the proxy-hierarchy to the guest institution and the user is granted access based on his permissions. A good example could be that the user is authorized to use the internet-connection on the guest site and is assigned in the guest-VLAN, based on the 802.1Q protocol. An overview of this situation is shown in the figure 6.

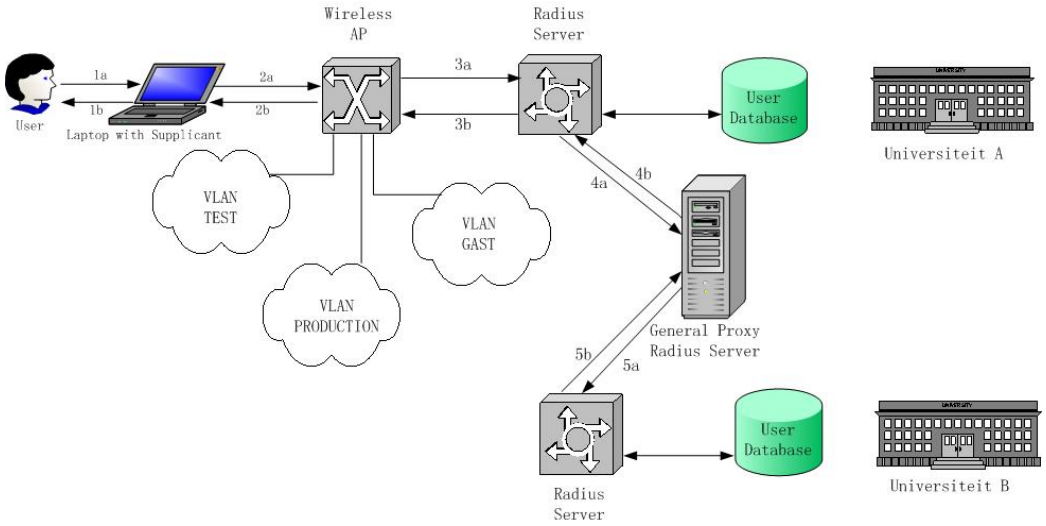


Figure 6: Working model for authentication of users within Eduroam system

In 6 the compete system infrastructure is showed. The application of the TAP-concept on this infrastructure is a little problematic. The examples of

the TAP-concept in [6] do not contain a situation that is comparable with this environment. We think that the TAP-concept does not anticipate (yet) on such special situations. In the TAP-concept, the Authentication and Authorization function of the security concept are draw as one single item. In the Eduroam example, this item consists of multiple components. In 7, this is pointed out as a square around the components involved. We will try to describe the security functions of the TAP-concept in the following subsections.

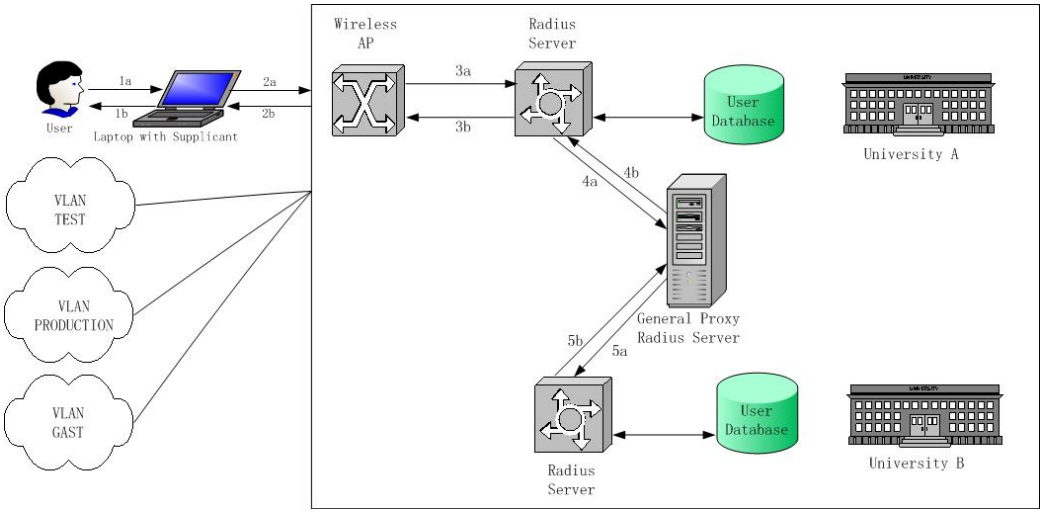


Figure 7: Working model for authentication of users within Eduroam system

5.2.2 Authentication and authorization

As shown in figure 8, the authentication function is only shown as one single element. This picture does not describe the complete environment according to us, but acctually complies with the trustmodels provided by the TAP-concept.

The authentication process is as follows:

1. (a) The user assumes that he communicates with the correct process (I&A)

   (b) The operating systems verifies the authentication of the user (I&A)

2. The user credentials are validated by the RADIUS Server, as described below

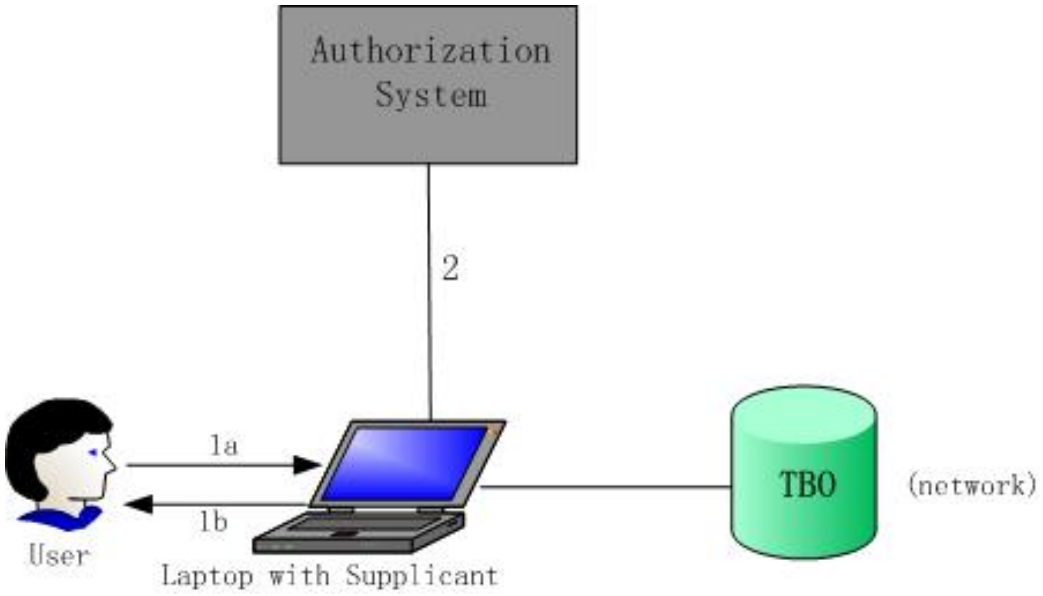


Figure 8: Overview of Trust relations for authentication between users and Eduroam System

The authorization process is as follows:

1. The user can use the computer after a successful log-on
2. The computer is placed in the correct VLAN after athorization with the RADIUS server(s), as described below

The user provides his credentials to the X-supplicant software (or these credentials are secure stored in the software). This softwaer is an additional module which passes the user credentials to the access point or switch. These credentials are then forwarded to the local RADIUS Server. This local RADIUS server discovers that it isnot responsible for the *@university-1.nl* realm and proxies it to the general RADIUS-proxyserver, this server forwards the credentials to the home-institution of the user where they are verified. The acknowledge of a successful authentication travels back over the proxy-hierarchy to the visited institution and the user is granted access. Because the user credentials travel via a number of intermediate servers, not under control by the home-institution of the user, it is important that the credentials are protected for privacy reasons. This requirement limits the types of authentication methods that can be used. Basically there are two categories of useful authentication methods, those that use credentials in the form of some public key mechanism with certificates (EAP-TLS, EAP-SIM) or those that

use so-called tunneled authentication (EAP-TTLS, PEAP). Authentication using both server and end-user certificates requires the roll-out of a public key infrastructure (PKI) with end-user certificates which has much overhead. Therefore it is also possible to use a tunneled authentication method that only requires server-certificates. (referenced from *Eduroam Goes Global - By James Sankar (UKERNA) and Klaas Wierenga (SURFnet)*)

5.2.3 Logging

The logging function cannot be desribed in previous picture, so we descided to show the logging function in the Eduroam-overview. This is shown in 9.

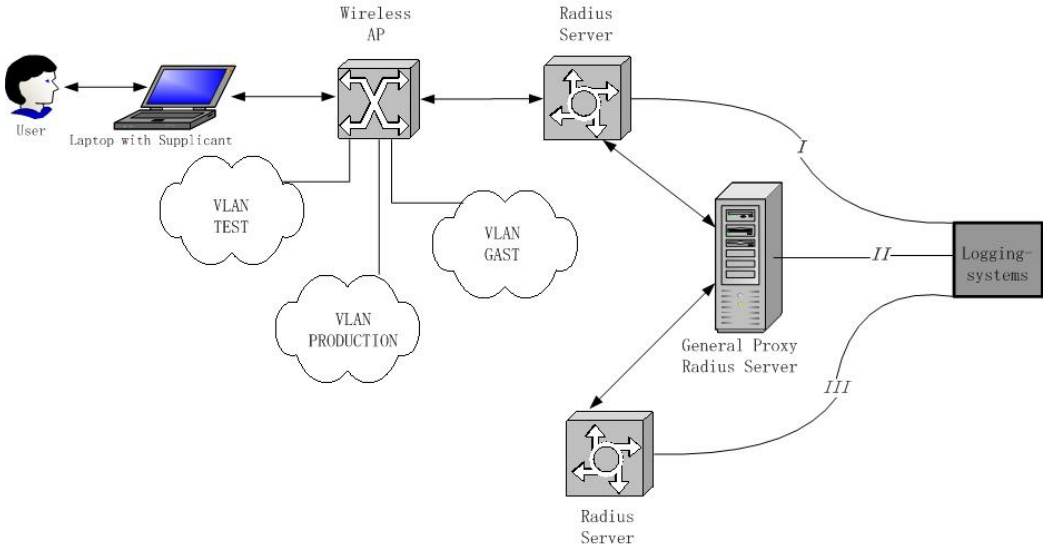


Figure 9: Overview of Trust relations for logging in the Eduroam System

1. All RADIUS Servers involved in the authentication and authorization log their actions to the general log facility

6 Conclusion and Recommendations

The TAP-concept is a very interesting concept. We learned a lot at the literature study of this concept. We think that this concept can be a successful addition to the concept that are already implemented at the TCA.

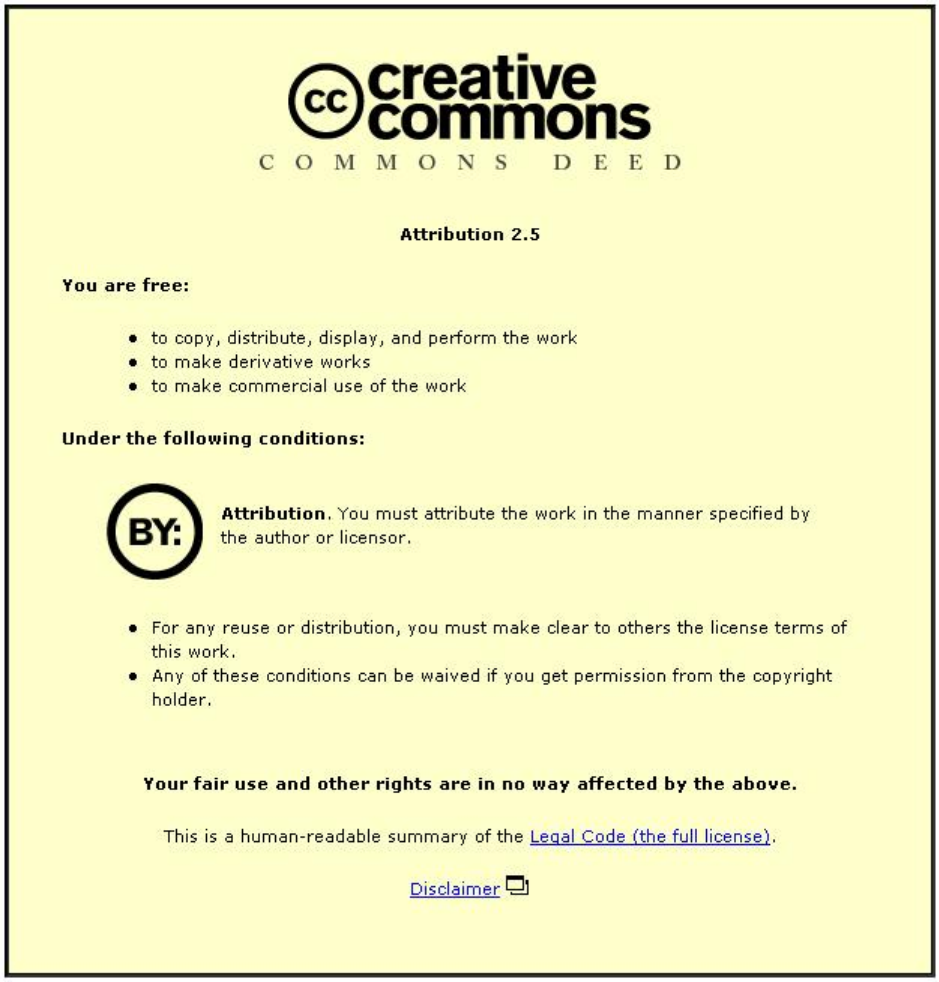
However, the application of the TAP-concept in the environment of the TCA will probably take a long time. To implement this concept, the requirements mentioned in this document, and the documents already available within the TCA, all describe that the main security functions authentication, authorization and logging should be implemented at an infrastructure level. This will require that all new applications are developed with implementatuib this concept, and that all old applications are converted so that they use these general security functions.

We think that the current definition of the TAP-concept does not anticipate on all environments yet. The TAP-concept should be able to desribe these special environments, containing access to other networks and extensive authentication and authorization structures, because the environment of the TCA is very large and comprehensive.

Also, as mentioned in the business requirements, the technical requirements are nog that interesting. The successful outcome of the implementation of this concept depends on the compliance with these business requirement. This business requirements are harder to archieve than the technical requirements.

7 Copyright Agreements

During the length of the project the following copyright agreements applies. For all documents the following *Creative Commons* license applies:



The full license is attached as Appendix A - Creative Commons Licence.

All possible source code deliverables are restricted by the BSD license limitation. The BSD license is attached as Appendix B - The BSD license.

References

[1] Website of System and Network Engineering
- `http://www.os3.nl`

[2] Website of the University of Amsterdam
- `http://www.uva.nl`

[3] Website of De Belastingdienst
- `http://www.belastingdienst.nl`

[4] Domeinarchitectuur, B/CICT Architectuur Scope 2004-2006, Domein Beveiliging, Versie 1.0 (3 maart 2005)

[5] ICT Service Scenario - Beveiliging/Vertrouwd Toegangspad, B/CICT Sector Architectuur

[6] Bijlage bij Addendum DA beveiliging 2000-2002, B/CICT-Architectuur, Trustrelaties voor het beveiligen van informatiesystemen, versie 1.0 (3 mei 2002)

[7] Eduroam information on website of Surfnet
- `http://aaa.surfnet.nl/info/eduroam/eduroam.jsp`

[8] 802.1X information on website of Surfnet
- `http://www.surfnet.nl/innovatie/wlan/crossdomain.shtml`

[9] Website of Eduroam.nl
- `http://www.eduroam.nl`

[10] Website of Eduroam.nl
- `http://www.eduroam.org`

Appendix A - Creative Commons Licence

Attribution 2.5

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.
BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

1. Definitions

   a. "Collective Work" means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this License.

   b. "Derivative Work" means a work based upon the Work or upon the Work and other pre-existing works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work will not be considered a Derivative Work for the purpose of this License. For the avoidance of doubt, where the Work is a musical composition or sound recording, the synchronization of the Work in timed-relation with a moving image ("synching") will be considered a Derivative Work for the purpose of this License.

c. "Licensor" means the individual or entity that offers the Work under the terms of this License.

d. "Original Author" means the individual or entity who created the Work.

e. "Work" means the copyrightable work of authorship offered under the terms of this License.

f. "You" means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from the Licensor to exercise rights under this License despite a previous violation.

2. Fair Use Rights.

Nothing in this license is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3. License Grant.

Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

a. to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;

b. to create and reproduce Derivative Works;

c. to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works;

d. to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audit transmission Derivative Works.

e. For the avoidance of doubt, where the work is a musical composition:

i. Performance Royalties Under Blanket Licenses.

Licensor waives the exclusive right to collect, whether individually or via a performance rights society (e.g. ASCAP, BMI, SESAC), royalties for the public performance or public digital performance (e.g. webcast) of the Work.

ii. Mechanical Rights and Statutory Royalties.

Licensor waives the exclusive right to collect, whether individually or via a music rights agency or designated agent (e.g. Harry Fox Agency), royalties for any phonorecord You create from the Work ("cover version") and distribute, subject to the compulsory license created by 17 USC Section 115 of the US Copyright Act (or the equivalent in other jurisdictions).

f. Webcasting Rights and Statutory Royalties. For the avoidance of doubt, where the Work is a sound recording, Licensor waives the exclusive right to collect, whether individually or via a performance-rights society (e.g. SoundExchange), royalties for the public digital performance (e.g. webcast) of the Work, subject to the compulsory license created by 17 USC Section 114 of the US Copyright Act (or the equivalent in other jurisdictions).

The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. All rights not expressly granted by Licensor are hereby reserved.

4. Restrictions.

The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

a. You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy or phonorecord of the Work You distribute, publicly display, publicly perform, or publicly digitally

perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this License. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any credit as required by clause 4(b), as requested. If You create a Derivative Work, upon notice from any Licensor You must, to the extent practicable, remove from the Derivative Work any credit as required by clause 4(b), as requested.

b. If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or any Derivative Works or Collective Works, You must keep intact all copyright notices for the Work and provide, reasonable to the medium or means You are utilizing: (i) the name of the Original Author (or pseudonym, if applicable) if supplied, and/or (ii) if the Original Author and/or Licensor designate another party or parties (e.g. a sponsor institute, publishing entity, journal) for attribution in Licensor's copyright notice, terms of service or by other reasonable means, the name of such party or parties; the title of the Work if supplied; to the extent reasonably practicable, the Uniform Resource Identifier, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work; and in the case of a Derivative Work, a credit identifying the use of the Work in the Derivative Work (e.g., "French translation of the Work by Original Author," or "Screenplay based on original Work by Original Author"). Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Derivative Work or Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5. Representations, Warranties and Disclaimer

UNLESS OTHERWISE MUTUALLY AGREED TO BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE WORK, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

6. Limitation on Liability.

EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE
LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. Termination

   a. This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Derivative Works or Collective Works from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.

   b. Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

8. Miscellaneous

   a. Each time You distribute or publicly digitally perform the Work or a Collective Work, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.

b. Each time You distribute or publicly digitally perform a Derivative Work, Licensor offers to the recipient a license to the original Work on the same terms and conditions as the license granted to You under this License.

c. If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

d. No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

e. This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Licensor and You.

Appendix B - The BSD license