Analysis of authentication systems
Which is the most suitable for BTG?

Adnan Hannani
Eva Johansson
Analysis of authentication systems
Which is the most suitable for BTG?
Adnan Hannani
Eva Johansson

Summary

The purpose of this project is to evaluate different authentication systems that make the authentication for remote VPN and Web users more secure. The purpose is also to recommend one system that we find suitable according to BTG’s requirement and network environment.

BTG Pulp & Paper Sensors AB is one example of a company where the remote users are using static passwords when they authenticate to the company network, and have now realized that it is time to make some changes since it is not secure enough. To make the authentication more secure, a system that automatically generates new passwords, at each login, is needed.

This report evaluates ActivCard AAA server, CRYPTO-Server, SecureID5.2, Premier-Access, and VACMAN server that provide strong authentication with dynamic passwords that are generated by a handheld device.

The evaluation is based theoretical study with information from the homepages of the system and by interviewing consultants, resellers and distributors. All requirements that BTG had and the other attributes that we found interesting to evaluate were compared to the information that we had about the systems.

All systems that we have evaluated are very similar in the way they perform the authentication process, but it was only ActivCard AAA server and SecureID5.2 that fulfilled all the requirements that were set up in cooperation the IT-unit at BTG. Since the purpose was to recommend one authentication system we used our attributes to select the most suitable. Our conclusion is that ActivCard AAA server is the most suitable. ActivCard AAA system advantages compared to SecureID5.2 is that the token can be resynchronized and have a longer lifetime. ActivCards uses a strong authentication technology since it combines the time and event synchronization and the system is also less expensive compared to SecureID5.2.
Acknowledgments

We would like to thank BTG Pulp & Paper Sensors AB for the opportunity to do our exam work at their company, which has been very informative. A special thank to our instructors Tord Larsson-Steen, Johan Lindmark and Jonas Nyman who have supported us during our study.

We also would like to thank all the resellers and distributors that we had contact with during our study; this has given us a deeper understanding of authentication systems.

From the University, we would like to thank our instructor Christian Ohlsson and examiner Thomas Lundqvist for their guidance during our study.

This report is for both technical and non technical persons. As the paper is going to be read by the economic department in BTG it is important that the content is easy to understand and gives a general picture of the problem and the solutions to come.
Contents

Summary....................................................................................................................................................i
Acknowledgments ...........................................................................................................................................ii
1 Introduction...............................................................................................................................................1
   1.1 The company BTG ..........................................................................................................................2
   1.2 Problem area ....................................................................................................................................2
   1.3 Purpose ............................................................................................................................................3
   1.4 Limitations .......................................................................................................................................3
   1.5 Report overview ............................................................................................................................4
2 Data security ............................................................................................................................................5
   2.1 Definition ........................................................................................................................................5
   2.2 Reduce potential threats ...............................................................................................................5
   2.3 Authentication ..............................................................................................................................6
   2.4 Authentication process ...............................................................................................................6
   2.5 Problems with static passwords .................................................................................................7
3 Strong authentication .............................................................................................................................8
   3.1 One-time passwords ...................................................................................................................8
   3.2 Authentication with tokens .......................................................................................................8
4 Methodology...........................................................................................................................................13
   4.1 Research methodologies ..........................................................................................................13
   4.2 Chosen method ..........................................................................................................................14
   4.3 Routine ..........................................................................................................................................14
   4.4 Internal interview .......................................................................................................................15
   4.5 Market analyse ..........................................................................................................................15
   4.6 Fact table ......................................................................................................................................15
   4.7 External Interview .....................................................................................................................15
   4.8 Selection .......................................................................................................................................16
5 BTG .......................................................................................................................................................17
   5.1 Current network ..........................................................................................................................17
   5.2 Components that is used .........................................................................................................18
   5.3 BTG remote Users .....................................................................................................................19
   5.4 How the remote user establish a connection ...........................................................................20
   5.5 The intended network ..............................................................................................................22
6 Requirements ......................................................................................................................................23
   6.1 System requirements ...............................................................................................................23
   6.2 Other attributes ..........................................................................................................................25
7 Result ....................................................................................................................................................28
   7.1 Selection of products ...............................................................................................................28
   7.2 Examined systems ....................................................................................................................29
   7.3 System overview .......................................................................................................................30
   7.4 Comparison results and analysis .............................................................................................31
8 Conclusions .........................................................................................................................................41
References .................................................................................................................................................42
Other references ......................................................................................................................................43
List of abbreviations
Here is a description of definitions and abbreviations that are used in this report.

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3DES</td>
<td>Triple Data Encryption Standard uses three stages of DES which makes it much more secure and suffices for most applications. Uses 168 bit key length.</td>
</tr>
<tr>
<td>AES</td>
<td>American Encryption Standard, a substitute to DES as an official American standard for encryption.</td>
</tr>
<tr>
<td>AD</td>
<td>Active Directory. An integral part the of Windows 2000/2003 architecture. Centralized and standardized system that automates network management of user data, security, and distributed resources, and enables interoperation with other directories</td>
</tr>
<tr>
<td>Authentication</td>
<td>To verify that the information comes from a trusted source or if the person or users are how they say they are</td>
</tr>
<tr>
<td>Bit</td>
<td>Binary digit. Smallest unit of data in a computer.</td>
</tr>
<tr>
<td>BTG</td>
<td>BTG Pulp &amp; Paper Sensors AB. BTG is the name of the company name and not an abbreviation.</td>
</tr>
<tr>
<td>Client</td>
<td>A “customer” that demands services from the servant (Server)</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard, a symmetric algorithm with 56 bit key length.</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized zone. A local network that doesn’t belong either to the internal network or the open Internet. In this local network, computers can be placed that in some circumstances can be reached both from Internet and from the internal network.</td>
</tr>
<tr>
<td>Dynamic password</td>
<td>Passwords that frequently changes</td>
</tr>
<tr>
<td>F</td>
<td>Fail.</td>
</tr>
<tr>
<td>Https</td>
<td>Hypertext Transfer Protocol over Secure Socket Layer</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol. Software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network</td>
</tr>
<tr>
<td>N/A</td>
<td>Not available.</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
</tbody>
</table>
| **Analysis of authentication systems**
| *Which is the most suitable for BTG?*

| **P** | Pass |
| PIN | Personal Identification Number. A typical number at four to eight digits. |
| **Password** | Can be a word, digit or a combination of both. Password is to authenticate identity of a person. Only the person knows the password. |
| **Remote Access** | Enables possession to the company’s network from an external place. |
| **RSA** | The enterprise RSA Security Inc. founded by Rivest, Shamir and Adelman 1982, then like RSA Data Security |
| **SMS** | Short Message Service |
| **Staff list** | Price list for product, prices depends on quantity. |
| **Tokens** | Handheld device that generates One-time passwords. |
| **IPsec+IKE** | Internet Protocol Security with Internet Key Exchange |
| **IT-unit** | Internet Technology unit |
| **URL** | Uniform Resources Locator |
| **USB** | Universal Serial Bus |
| **Username** | Unique name for a person can be word, digit or combination of both, often to verify the identity of the person. Username is often combined with password. |
| **Validation** | To verify if the person, asking to access the network. |
| **Verisec** | Consultant company in Stockholm, reseller for ActivCard, RSA, Secure Computing and Vasco |
| **Virtual Private Network** | Uses an open, distributed communication channel like Internet, to secure the transfer of information. |
| **VPN** | See Virtual Private Network |
| **WWW** | World Wide Web |
List of figures and tables

Figure 2.4.1 Traditional authentication process
Figure 3.2.1 Challenge-Response user step in a login procedure.
Figure 3.2.2 Time-dependent user steps in a login procedure.
Figure 3.2.3 Event-dependent user steps in a login procedure.
Figure 5.1.1 Overview over current VPN-traffic and authentication flow at BTGs headquarters.
Figure 5.4.1 BTG’s network environment at one office location.
Figure 5.5.1 Example over how the VPN-traffic and authentication flow between BTGs headquarters can look like after centralization
Figure 7.3.1 How the BTG network environment can look after the implementation.

Table 7.1.1 Description over table, categories and evaluation queries
Table 7.2.1 Producers, systems and their addresses.
Table 7.4.1 Description of platform, applications, VPN.and Web users.
Table 7.4.2 Support and warranty of the systems.
Table 7.4.3 Support for authentication devices and token features.
Table 7.4.4 Authentication modes and data encryption.
Table 7.4.5 Cost analyses for the systems.
1 Introduction

Internets rapid development makes it possible for the private and public sector to communicate and distribute data, which can be any kind of information e.g. Word and Excel documents, in a more efficient and easier way than before. The development of internet has contributed to reach a bigger global market than ever before. Both the private and public sector see possibilities to open up their systems for their distance workers. For example employees, suppliers, and customers can work more efficiently by giving them access both to the confidential and non-confidential information on the company network. As the information today is the key factor for both private and public sector, it is essential to keep it safe, but as known both the employee and the company management can often be careless with security issues (Good Bengt, 2000).

To secure the local network and to keep the information safe the users must identify themselves to the company network. This to secure that the user has access right. Open systems for distance users will increase the demands on the company’s security policy, to handle user authentication in a more sufficient and secure way.

The purpose of the authentication process is to confirm the identity of the user in a system. This is often done by proving something e.g. ones identity (username), and something known only to the user, proof of identity (password).

There are various methods for the users to prove their authority but the most common one is username and static password.

Static passwords are the weakest form of proving ones identity. Such passwords can easily be guessed, stolen or otherwise compromised and it is therefore important that one frequently change ones password. On the other hand, the disadvantage of frequently changing the password contribute to higher workload for the system administrator as he or she has to change all current passwords to new ones, and determine if the user has acknowledged the new password that has been given. It can also be a security risk, with frequently changing passwords, as the users have to memorize new passwords again.
1.1 The company BTG

BTG Pulp & Paper Sensors AB is one example of a company who is using static passwords but has now realized that it is time to make some changes in the most critical areas.

BTG is situated in several countries and has a lot of information that should be reached by both local- and distant employees that belongs to BTG. To make this possible BTG uses both VPN\(^1\) and Web access services. These services are only open to those who are entitled to access confidential information outside the home network.

To access these services the employees have to go through a login procedure where they have to make an identification and authentication with username and static password. This is a security risk, since password alone cannot ensure secure remote access.

1.2 Problem area

As we said earlier the authentication process with static passwords is a problem because it is the weakest form of authentication and can easily be guessed, stolen or otherwise compromised. Therefore, the use of a static password is not appropriate for a remote access connection to the company’s network. But still, it is widely used and the main reason could be because an authentication process with static password is easy to deploy and is inexpensive.

BTG believes that the use of static passwords, in the authentication for establishing a connection via VPN- and Web access services, is a weak point. They also find it hard to administrate the need of frequently changing the static passwords and to be sure that the distant workers have observed that they have been given a new one, by e.g. mail, since they do not have a proper way to process it.

What BTG needs is a system that automatically process the frequent changes of passwords, without any interference from the administrator, and at the same time make it easy for the user to always know the correct password. The password should be a one-time password and be generated by a handheld device, a hardware token, which displays the correct password for each login attempt.

Such an authentication system will increase the security to the VPN- and Web access authentication since the password is different at each login attempt. This solution minimizes the risks of exposing the password, since it only can be used once, and results in less administrative work since manual changes of passwords are avoided. Further advantages of this solution are that the users do no longer have to memorize new password and they can no longer be written down.

\(^1\) A virtual private network (VPN) is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network

2
There are many different types of authentication systems on the market so the problem is to find the authentication system that follows BTG’s requirement and is the most suitable according to the current network environment.

1.3 Purpose

The purpose to this work is to find the most suitable system that process the authentication before a secure established connection via VPN- or Web remote services can occur to BTG’s network. Our intention is to look at different types of systems that solve the insecurity with static passwords for the authentication procedure and to evaluate which of them is the most suitable according to BTG’s requirement.

1.4 Limitations

We have chosen to not make any detailed study of protocol, algorithms and technologies since this is not included in our extent of report. We have also chosen to not make any study of the following statements

- Biometric authentication. BTG finds that biometric authentication is still too un-explored and new technology to be considered at this moment.

- Mobil phone (SMS authentication). The problem with SMS authentication can be if users are in remote area with no wireless coverage e.g. in a basement. This is one of the main reasons why BTG does not find it suitable.

- Smart card authentication. Smart cards require a card reader which means that the user has to carry an extra unit. There will also be more administrator work-load since they have to install a driver on each workstation which also makes the system less flexible since one can only logon to workstations with this drive installed.

- Certificate authentication. Like Smartcards, certificates require more administration in terms of installation of the certificate on the client.

- Firewall (Validation and filtration). This stage comes after the authentication and does not affect this report.

- The result will only consider one office or location. However, our recommended authentication system will be possible to use on all BTG’s offices and locations if that’s desirable.

- This is only a theoretical study and do not include tests or installations. The reason for this is that BTG wanted a brief theoretical overview over a suitable product that can be used. Since no tests are made, it will be hard to evaluate the user-friendliest of the systems.
1.5 Report overview

Here is an overview over the report, this to make it easier for readers that are interested in specific chapters.

**Chapter 1 – Introduction.** Gives an overview over the background, purpose and limitations of the project.

**Chapter 2 – Data security** This chapter describes the definition of data security, how to reduce potential threats, authentication and its process and why it is problem with static passwords.

**Chapter 3 – Strong authentication** This chapter describes what strong authentication is and different authentication modes that can be used to secure the user identity.

**Chapter 4 – Methodology** An overview over the methodology, and the methods were used to gather the information that was needed.

**Chapter 5 – BTG** Gives an overview over BTG’s network environment, the components that are used to establish a VPN and Web connection to BTG and how the users establish a remote connection. It also gives an overview over the intended network.

**Chapter 6 – Requirements** A list of requirements and attributes that the system has to support.

**Chapter 7 – Result** Specifies the systems that are analysed and how well they supported the requirements and attributes that were set up.

**Chapter 8 – Conclusion** The conclusions that we have drawn from the result.
2 Data security

This chapter introduces the area of data security, explaining the definition of data security, how to reduce the potential threats, authentication, the authentication process and the problems with static password. Readers with a good knowledge of data security can skip this part and go on to Chapter 3.

Further reading about data security can be done at, Säkerhetsarkitekturer, 1999, by SIG Security.

2.1 Definition

The definition of data security comes from ITSEC (Information Technology Security Evaluation Criteria) and comprises three aspects (Säkerhetsarkitekturer, 1999). These aspects are confidentiality, integrity and availability. Confidentiality is about to prevent someone getting access to the information without permission. This includes both reading, changing or makes conclusions of the content. Integrity is about prevent, illicit modification of information. One wouldn’t want anyone to make undesired modification of current information, delete information or enter new information that hasn’t been there before. Availability is about services, that they must be available when they are desired, without any unnecessary delay.

2.2 Reduce potential threats

With worldwide connections, networked computers are vulnerable to hacker attacks 24 hours a day. The Internet allows the electronic equivalent of an intruder who looks for open windows and doors. Now, a person can check for hundreds of vulnerabilities in just a few hours.

By adding a remote access VPN, e-mail gateway or World Wide Web (WWW) site, that employees can access while away from the office, companies may unwittingly provide a "back door" into their computer network. To reduce these risks of providing a “back door”, many strong tools are available.

A firewall is the point at which a private company’s network and a public network, such as the Internet, connect. A firewall system is a hardware and software configuration which sits at this perimeter, controlling access into and out of a company's network. While in theory firewalls allow only authorized communications between the internal and external networks, new ways are constantly being developed to compromise these systems. However, properly implemented they are very effective at keeping out unauthorized users and stopping unwanted activities on an internal network.
Firewalls also have functionalities such as encryption and VPN capabilities. Encryption is the coding or scrambling of data and keeps unintended users from reading the information. VPN employs encryption to provide secure data transmissions over public networks such as the Internet. Even though VPN provides secure data transmission it is not completely secure without authenticity of users.

### 2.3 Authentication

Authentication is a process where the system confirms the identity of a user, requesting access to computers, networks or computerized resources. The most common form of authentication is when a person uses a username and a password. The password should only be known to the user and to the system. (searchSecurity, 2004)

### 2.4 Authentication process

Beside the actual password verification and users right (authorization) management, one also needs number of services available for the users (Vasco, 2004). Schematically this can be represented as in Figure 2.4.1

![Figure 2.4.1 Traditional authentication process, (figure drawn and modified from Vasco, 2004)]
User authentication

The user authentication application is responsible for checking the user-id and the password that has been given by the user or administrator. The verification process of user id and the static password are based upon the comparison of the given static password with the password stored inside a database. If the password matches the password inside the database, the User Authentication module returns a YES. If the password does not match, the module returns a NO. Based upon the return code YES or NO the user will be granted access to the application.

User management

The user management function is to allow one to add new users to the system. One gives specified information about the user such as user-id and password along with specific rights for the system. The user management must be secured so no unauthorized person can access it to make changes in existing accounts or create new accounts.

Administration

Inside the Administration application a number of administrative tasks can be found, such as password management rules. For example, the rules can be that users must change their passwords every 45 days or passwords need to be at least 6 characters long and must include some digits.

2.5 Problems with static passwords

Since today’s society is characterized by having many passwords for different things, e.g. credit cards and user accounts, users can have problem to memorize them and must write them down on a piece of paper. This is mostly because the passwords, which are given to the user, are of random nature with no logical sense. If the user picks his or hers own password, they are likely to choose an easy one that is related to them personally e.g. a date of birth, a telephone number and so on. By doing this they jeopardized the security that the password gives.

To solve this problem companies, Internet banking and many other transactions requires strong authentication. (searchSecurity, 2004)
3 Strong authentication

Strong authentication (SecureComputing, 2004) is when a system requires multiple factors for authentication and use advanced technology, such as dynamic passwords before authorizing the user access to the system. There are numerous kinds of systems that can be implemented, and one of them is the use of a token (Fcw.com, 2004). The token generates one time passwords, and can be found in various forms like credit cards, key chains or like a small calculator.

An example of multi-factor authentication can be ones internet banking. This requires something one have (token), and something one know (PIN to the token).

3.1 One-time passwords

One time passwords are, as the name implies, passwords that only can be used once. This means that even if someone is eavesdropping on the network, they will not be able to make use of the passwords they steal unless they have a very effective decryption program or the one-time password encryption algorithm is very week.

3.2 Authentication with tokens

The main purpose for hardware token is to generate one time passwords and to overcome the traditional static passwords. The token is personally assigned to the user, this to prove the users identity to the specific token. Without the correct token the user is unable to access the system.

There are four basic types of authentication modes that can be used with tokens, asynchronous and synchronous, with or without PIN. The biggest difference between them is that asynchronous authentication using challenge-response and synchronous authentication is using time and event synchronization. (SecureComputing, 2004)

3.2.1 Asynchronous authentication

Asynchronous authentication is often called challenge-response (Unicenteradvisor, 2004). In this implementation the authentication server sends a challenge to the user. The user then generates a response, one-time password, for the challenge by using the token. The one-time password is then sent to the server. The server then compares the password by using a secret key that is shared with the token and either confirms or refuses the user’s identity. In challenge-response authentication is done in 5-steps. These steps can be viewed in Figure 3.2.1.
Analysis of authentication systems
Which is the most suitable for BTG?

Figure 3.2.1 Challenge-Response user step in a login procedure (rsasecurity, 2004)

Information about the advantages and disadvantages with Challenge-response is collected from documentation from SecureComputing’s homepage.

Advantages with Challenge-Response:
- No synchronization is required since the server only matches the response with the secret key that is shared with the token.
- Dynamic passwords can be shorter since they frequently are replaced by a new one and the risk of being stolen is minimal.
- Easy to understand by all kind of users, e.g. sales man, administrator etc.
- Exhaustive password attacks are difficult to perform because each and every access attempt begins with a new random challenge, so the attacker must start a brute force password attack from scratch each time.

Disadvantages with Challenge-Response:
- Many steps for the users since they first have to enter the challenge into the token and then have to enter the answer into the login page.
- Some protocols and client applications don’t support challenge-response e.g. some routers, VPNs and firewall.
3.2.2 Synchronous authentication

A synchronous password is as strong as an asynchronous password, and it requires fewer steps between the client and server compared to a challenge-response process. The synchronous token do not require user to enter any challenge, since no one is given from the server. This makes synchronous tokens easier to use. Synchronous tokens are time or event synchronized, or a combination of both, with the server. (Unicenteradvisor, 2004)

In a synchronous password implementation one have a dynamic variable that can be either time (clock) or event (counter) based, or both, and a secret key that is shared between the token and the server. The token generates the synchronous password by using the variable and the shared secret key. The password is then sent to the server. The server then compares the password with its own password, and then either confirms or refuses the user's identity.

**Time-dependent synchronization**

Time-dependent synchronization has to have a clock present both in the token and the server. Both the server and the token take the current time as the input value, e.g. every 30 or 60 seconds the token read the time from its clock and use it as the input value to generate a password. The current time is an encrypted input value using the user's secret PIN as part of the authentication process. The result is one-time password. (SecureComputing, 2004)

An overview over the user steps in time synchronization can be viewed in Figure 3.2.2

![Figure 3.2.2 Time-dependent user steps in a login procedure (SecureComputing, 2004)](image-url)
Information about the advantages and disadvantages with Time synchronization is collected from documentation from SecureComputing’s homepage.

**Advantages with Time-synchronization:**

- Like Challenge-response, it is difficult to perform exhaustive key attacks, in time synchronization, since the password only is valid for a certain amount of time.
- More compatible with e.g. routers, VPNs and firewalls, as there is no challenge involved.
- Easier to use than challenge/response since fewer user steps is required to authenticate.

**Disadvantages with Time-synchronization:**

- Administrator may have to resynchronize the server if the clock on the tokens drifts.
- Users have to wait some time if they enter wrong password. Can be up to 60 seconds.
- High battery consumption, because the token is always on.

**Event-dependent synchronization**

Event synchronization (SecureComputing, 2004) does not rely on an internal clock as the time-dependent, but instead it uses a simple counter as an input value. When a token is used for the first time, the internal counter is set to zero. When the user requests a new password by entering the PIN, the counter is incremented and the incremented value is used as an input value. The one-time password is an encrypted value. Like the token, the user account also contains a counter at the server. This counter is initialized to zero when the account is created, and is incremented every time the user is authenticated.

Event synchronization is easier to keep synchronized since the server can maintain synchronization between the two counters by adjusting its counter to match the counter in the token. This can be useful if the user for some reason generates new passwords without using them for authentication.

An overview over the user steps in event synchronization can be viewed in Figure 3.2.3
Analysis of authentication systems
Which is the most suitable for BTG?

Figure 3.2.3 Event-dependent user steps in a login procedure

Information about the advantages and disadvantages with event synchronization is collected from documentation from SecureComputing’s homepage.

Advantages with user-Synchronisation

- Like Challenge-response and time synchronization, it is difficult to perform exhaustive key attack.
- Like time synchronization, it is easier to use than challenge/response since fewer user steps is required to authenticate.
- Like time synchronization, it is more compatible with e.g. routers, VPNs and firewalls, than challenge/response tokens.
- Do not require manual resynchronization for either administrator or users since the server manage this by its self.

Disadvantages with event- Synchronisation (SecureComputing, 2004):

- The user might write down the password on a peace of paper and allow them to be compromised.
4 Methodology

This chapter presents an overview over general methods that are used in research methodology and the methods that we have used to accomplish our goal.

4.1 Research methodologies

There are two different groups of methods that are used in research methodologies and these are the qualitative- and quantitative methods and will be described below.

Qualitative method

The qualitative method deliberatively gives up on quantity in order to reach a depth in analysis of the object that is studied. This research method relies on interviews, observations, and small numbers of questionnaires, focus groups, subjective reports and case studies which are some of the most important methods (yourencyclopedia.2004). The assumptions that are generated during the collection of information and analyse, and measurement tends to be subjective. In the qualitative approach, the researcher becomes the instrument of the collection of information, and the result may vary, depending upon who carries out the research. The advantage of using qualitative methods is that they generate detailed information that leaves the participants perspectives unchanged. A disadvantage in qualitative collection of information is, that difficult to draw meaningful conclusions from the gathered results as outcomes may vary rather inconsistently and time-consuming (social marketing, 2004).

Qualitative methods are commonly used in conjunction with quantitative methods. By using qualitative methods it is often possible to understand the meaning of the numbers produced by quantitative methods.

Quantitative method

Quantitative research methodology is the opposite to the qualitative research methodology, which tends to be more focused on the collection and analysis of numerical data and statistics. Quantitative research method is designed to ensure objectivity, generalizability and reliability. These techniques cover the ways research participants are selected randomly from the study population in an impartial manner, the standardized questionnaire or intervention they receive and the statistical methods used to test predetermined assumptions regarding the relationships between specific variables. The researcher is considered external to the actual research, and results are expected to be replicable no matter who conducts the research.
4.2 Chosen method

We have chosen to use the qualitative method since our study is based on information from the producer’s documentation and conversations with consults, resellers and distributors. These conversations couldn’t be based on strict questionnaire since there are other aspects that have to be considered. For example, the technicians have different experiences with these types of systems and they all have their own favourite, which means that all gives different type of answers to the same type of question.

Our result is being based from an objective point of view.

4.3 Routine

This part gives an overview over how our study was performed, and is done in the same manner as they are written below.

**Planning**

We prepared us by making some literature studies and discussions with our client to be able to define the problem. We then decided which methods we should use to accomplish our goal.

**Requirement analysis**

The base for this essay is the need that our company has to secure their network environment. To identify these problems, a number of interviews have been made with the IT-unit which resulted in what exactly they needed, how they handle the situation for the moment and number of requirements that the new system has to support.

**Market analyse**

By contacting resellers, distributors and searching information on the Internet, we obtained a picture of the kind of systems that could be suitable for our client.

**Product analyse**

Since there was no specific technical difference between the systems, we decided to do a further study on how well they support our client requirements.

**Evaluation**

At the end, the result from our study was put together and our own conclusions were made.
4.4 Internal interview

To be able to identify the company’s need of new remote authentication solutions for remote users, several internal interviews were made with the IT-unit at BTG. These interviews resulted in what kind of network environment and authentication system they have for the moment and what they would prefer instead to increase the remote authentication security (see chapter 5). The most important requirements that the system had to support, were put together with the IT-unit, this to be sure that the new system fulfils its purpose. These requirements can be viewed at chapter 6.1

4.5 Market analyse

When the company’s need was identified and put together, a market analyse could begin after systems that could fulfil the needs and requirements.

This analyse was made to find out what different kind of authentication systems that were available for the moment, and if they were suitable for this kind of purpose.

This analyse was mostly made on Internet but also by conversation with resellers and distributors of these kinds of systems.

The number of systems that we have chosen to study is (see table 7.2), according to the resellers, the most known for this kind of purpose, but we do not exclude that it can be other systems that are well qualified and suitable.

4.6 Fact table

Fact table was used to gather detailed information about the products, this to get a brief understanding over how the products worked, their features, their benefits and if they are compatible with the current network environment at BTG.

Most information is based from the producers own documentation at their homepages, this information was then compared with the requirements that were set up together with BTG and other attributes that we found interesting to evaluate.

For further information, which where not available at the producer’s homepages, we contacted resellers or consultant.

4.7 External Interview

To confirm or find out new information that could be useful for our study, interviews with consultants or reseller, that work with this kind of system, were done. These people were interviewed because they are very familiar with these kinds of systems since they have done several implementations in different network environments.

Information that consultants or resellers found necessary to know, to be able to answer our questions, was given during the conversation or by e-mail.
4.8 Selection

The selection was based on the requirements that were put together with the IT-unit at BTG (see Chapter 6.1). We also chose to take a further look at some other interesting attributes that we thought was important to the system to have (see Chapter 6.2). These requirements, including our own list of attributes, were divided into different priority levels, depending on how important it was that they were fulfilled.

A more detailed explanation over our product selection can be found in chapter 7.1.

All our statements are based on producers own system documentation and conversations with consults and resellers.
5 BTG

The following part of this section will describe which types of remote users BTG has, how they establish their connection via VPN or Web to the network and which components that are involved. All information about BTGs network environment and applications has been gathered through meetings with Tord Larsson-Steen and Johan Lindmark from the IT-unit at BTG.

5.1 Current network

The current situation at BTG is that they have headquarters in Sweden, Switzerland, Germany, USA and smaller offices in several other countries see Figure 5.1.1.

Figure 5.1.1 Overview over current VPN-traffic and authentication flow at BTGs headquarters.
Every country takes care of their own Local Area Network (LAN) and Demilitarized Zone\(^2\) (DMZ), which means that every country takes care of its own distant worker and the administration of their user accounts. Between these countries is one VPN-tunnel established that is mostly used for updating virus protection and Active Directory (AD) replicating.

All users that are going to establish a VPN or Web connection must authenticate themselves at their country that they belong to.

### 5.2 Components that is used

To be able to establish a connection there are components that has to be used to make this possible. In this section will we give a short overview over these components.

#### 5.2.1 VPN protocol VPN client (checkpoint secure client)

All users that are entitled to the VPN have a VPN-client, checkpoint secure client, installed on there laptop, this is a combination of a personal firewall and authorization client to the VPN network. The personal firewall is to protect the otherwise unprotected user that is about to establish a VPN connection.

#### 5.2.2 Web application

To make a Web connection, there is no specific component that has to be used except that one needs to have a browser of any type.

The web application uses https (Hypertext Transfer Protocol over Secure Socket Layer) to encrypt and decrypt user page requests as well as the pages that are returned from the Web server.

---

\(^2\) DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data.(whatis, 2004)
5.3 BTG remote Users

BTG has chosen to classify their distant users in three different categories. These categories are grouped after what they are allowed to access at BTG, via a remote connection.

We are going to make a brief explanation of these categories of remote users.

- **VPN-user**
  This user is entitled to have remote access to the LAN which means that they can access their files wherever they are at the moment. All VPN-users has a VPN-client installed on their laptop. This client lets them establish a secure connection directly to the BTG firewall over the Internet which makes it look like their laptop is a workstation at the local network.

- **Web-user**
  This user is only entitled to access the DMZ, and not the LAN at the BTG network. The user can access the DMZ wherever they are by accessing the Internet and log on at BTG service site.

- **All other users**
  This is the user that visits the BTG home page where public information can be found about the company. The service site is a public site where no restriction of users is set. This user will not be further discussed in this report since there is no need for any authentication.
5.4 How the remote user establish a connection

As we mention earlier there are three different categories of remote users, but we are only going to examine two of them, VPN- and Web remote user.

In this section will we only going to examine how the connection is established between the remote user and the company network. There will only be a schematic overview of one office since they all work in the same manner see Figure 5.4.1.

Figure 5.4.1 BTG’s network environment at one office location.

VPN-user

1. All VPN users have a VPN-client installed on their computer. This client has to be activated before an authentication attempt can occur.

2. To establish a VPN-tunnel, the user must enter their username and static password at the client’s login prompt. When the authentication request reaches the firewall, (CheckPoint VPN-Ing) a validation of the user will be made to see if the user has access rights or not. If the user has entered a wrong username or password, no access will be granted.
To verify the authorization and connection without exposing the information, Internet Protocol Security with Internet Key Exchange (IPsec+IKE) is used.

3. When the user is successfully authenticated, a VPN-tunnel will be established between the user and the company’s firewall to secure the data traffic.

4. A local authentication at the AD can now be made, to get access to their local user account.

**Web-user**

A. To access the service site, the user has to log on via a web application. They access this application by typing the service-site Uniform Resources Locator (URL) address in a Web browser to the Web server.

B. When the firewall Checkpoint VPN-1ng notices the request of accessing the DMZ, it makes a Network Address Translation (NAT) and redirects it to the DMZ.

C. The log on procedure is with username and static password, it is validated at the authentication server in DMZ, so there is no validation at the firewall, neither has the user-database access to BTG’s AD service.

D. Once the user has been validated in the user database, they get access to the information that they are entitled to at the DMZ. But as the Web users are directed to the DMZ, they do not have access to the company’s LAN like VPN users have.
5.5 The intended network

During this year BTG will go through big changes as they are going to centralize the Internet Technology unit (IT-unit) to Sweden.

The thought is that all BTG-users that are going to establish a connection, independent on which country they belong, have to go through Sweden and then be redirected to their respective country via VPN-tunnel (see Figure 5.5.1), that is as they want to have more control over the users that access the network and to minimize the risk of being hacked. This can seem to cause traffic congestion but that is not likely because of the users different locations with different time zones there will not be any problem since they will not access the server at the same time.

Figure 5.5.1 Example over how the VPN-traffic and authentication flow between BTGs headquarters can look like after centralization.
6 Requirements

This chapter describes the requirements that BTG demands that the recommended system has to follow and other attributes that we found important to take a further look at. This is to make sure that the system is compatible with the current network environment and that it fulfils the intended purpose. All system requirements, except other attributes, have been gathered through meetings with Tord Larsson-Steen and Johan Lindmark from the IT-unit at BTG.

The requirements are given a priority level to specify the importance of the feature. It is from these priority levels that the result will be based on.

The priority levels are: Critical, High, Medium and Low.

Critical

Have to be supported by the system. Systems that do not support these requirements are not suitable for BTG’s network environment and will therefore not be recommended.

High

These requirements are very highly prioritized and should be fulfilled. If systems have more than one failure or not available (N/A) in this priority level, they will not be recommended.

Medium

These requirements are desired to be fulfilled. The requirement is not essential for the system, but it will be essential for the system we choose.

Low

These requirements are desired, if they can be fulfilled, but they are not essential for the system or the selection of the system.

6.1 System requirements

The following requirements are set by cooperation with BTG

- Windows 2000
  Compatible with windows 2000 server, the underlying computer system on which application programs can run. BTG’s platform today is based on Windows 2000. To minimize the administration workload and to keep the network environment more standardized it has to be required. Since Windows 2000 is a requirement that has to be fulfilled, we define this requirement as critical.
Analysis of authentication systems
Which is the most suitable for BTG?

- **Windows 2003**
  Compatible with Windows 2003 server. BTG is planning to change their platform in the future to Windows 2003 so the product has to support this platform, this to keep the administrator workload down and keep it standardized in the whole network environment. Windows 2003 is also a requirement that has to be fulfilled, so we define this as a critical requirement.

- **Microsoft Exchange 2003**
  Microsoft Exchange 2003, a server application for handling message and group communications. BTG uses for the moment Exchange 5.5 but are now upgrading to Exchange 2003. This requirement is set to medium as it does not have to be fulfilled. But if the systems support Exchange 2003 it would be good.

- **Check Point VPN-1**
  BTG is using the Check Point VPN-1 today and has no plans to change this, as they are very satisfied with it. So the validation products have to be compatible with Check Point VPN-1, that’s why the requirement is set to critical.

- **LDAP**
  LDAP (Lightweight Directory Access Protocol), software protocol for enabling anyone to locate e.g. organizations, individuals and other resources such as files and devices in a network. To communicate between authentication servers LDAP must be supported and have the requirement set to critical.

- **Active Directory**
  Active Directory, a centralized and standardized system that automates network management of user data, security, and distributed resources. BTG uses Active Directory so the requirement is set to critical.

- **VPN- and Web users**
  BTG have both VPN- and Web-users; the new authentication system has to support both kinds of users. This means it has to work for VPN- and Web clients. Therefore the requirement is set to critical.

- **Event log records**
  Keep log records of authentications, whether they are succeeded or not. This is important when evaluating attack attempts, so we define this requirement to critical.

- **Lock user account**
  User accounts must be locked when too many logon attempts are made without any success. If there is no lock, anyone could try to access the network via brute force. We find it to be a critical requirement.
Analysis of authentication systems
Which is the most suitable for BTG?

- **Token with PIN**
  Hardware token with PIN that generates one-time passwords. This to verify that it is the right user that uses the token. The requirement is set to high since it is still a strong authentication without PIN.

### 6.2 Other attributes

These attributes are set us to make a thorough analyse of the systems.

- **Mixed network**
  Compatibility in mixed network so that the system can run on other systems than Windows, like UNIX, SUN. This is if BTG in the future decides to change or add some new applications to their network. This level is set to low as BTG is only using Windows product and have no plans to change the network environment.

- **Support**
  Support for users and administrators. If they have any problems with the software or the token after the system implementation. The priority level is critical so if the user or administrator call the support, it is essential that they get the help without any delay or hassle.

- **Warranty**
  Warranty for software and token. If the token stops to work, the users must get a new token. Software is set to low as the upgrades and patches are included in maintenance. The token have medium level as there is more risk that they will stop working.

- **Variety of authenticators**
  Producer should have large variety of authenticators. This to extend the flexibility for the companies to test or change to different authenticators. The priority level is set to low, as the producers frequently develop new types of authenticators.

- **Token lock**
  If any unauthorized person tries to log in to the token to many times, the token should lock it self. This function is important if the user looses the token, that’s why it is set to level high.

- **Token unlock**
  The administrator or user should be able unlock the token if e.g. the user by mistake locks the token. The priority level is set to high, since the user cannot access its account.
• **Re-synchronization**  
The administrator should be able to re-synchronize the tokens if they drift or loses its count, instead of sending the token to the consultant or producer and lose time and money. To minimize the cost and time lose the priority level is set to high.

• **Change of PIN**  
Users should be able to change or to choose their own PIN. The level is set to medium since it can be security risk if the users have to easy PIN code

• **User deployment tool**  
Possibility for the users to write the information about them self in the database and get the token from administrator assigned to them. If the users are in remote place and have to have the token sent to them. Here the level is set to low regarding the security risk.

• **User-friendly**  
Token design should be user friendly and appealing either it can be placed on a key ring or have a credit card or calculator style. The priority level is set to low as this is not essential for the authentication or the system how they look or feel. It is also difficult to determine if the system is user-friendly since no practical test will be done.

• **Battery consumption**  
Battery consumption should be low so the users or administrator won’t have to replace them frequently. The level is medium regarding the cost aspect.

• **Token life time**  
Token life should be long so BTG won’t have to buy new token frequently this to reduce token cost. This priority level is set to low as BTG will have some tokens in reserve.

• **Replaceable batteries**  
Users or administrator at BTG should be able to replace the battery of token this to save time and administration of sending the token to the consultant or producer. To save time the level is medium.

• **Authentication mode**  
If the systems support various authentication modes for synchronous and asynchronous, that is time, event or challenge-response based it will make the system more flexible. That’s because BTG perhaps wants to change the way of authentication for some reason. The priority level is set to low as all the authentication modes are good and is strong authentication.
• **Data encryption**

Data encryption is to ensure the privacy, by hiding the information from persons it is not intended for. Even if the person can see the information it will understand it as the information is encrypted. When it comes to networks or internet the data encryption allows one to have secure communication over an insecure communication channel.

The standard of 128 bit long encryption key is good since a 128 bit long key contains $2^{128}$ different keys and if a hacker wants to break the 128 bit long key he will have to try half of the key combination to get lucky. This level is set to medium as the data encryption is important for the safety.
7 Result

This chapter describes how we state our requirements, the different systems that we have chosen to analyse and our result.

7.1 Selection of products

We have chosen to state all our analysed systems requirements in different tables. These requirements are divided into categories. The following table 7.1.1 shows in which table one can find the different categories, requirements and attributes that are going to be evaluated.

How well the system fulfils the requirements has been judged by a subjective point of view since the categories of a security system is hard to quantify.

Table 7.1.1 Description over table, categories and evaluation queries

<table>
<thead>
<tr>
<th>Table: Categories</th>
<th>Question to be answered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 7.4.1</td>
<td>Do they support the required platforms, applications and the different remote users?</td>
</tr>
<tr>
<td>Table 7.4.2</td>
<td>How the administrator can follow the logging.</td>
</tr>
<tr>
<td>Support</td>
<td>Different types of support the developer offer.</td>
</tr>
<tr>
<td>Warranty</td>
<td>How long time the software and token warranty last.</td>
</tr>
<tr>
<td>Table 7.4.3</td>
<td>Types of authentications the system support. Type of encryption. If the user account will automatically lock when too many unsuccessful login attempts occur.</td>
</tr>
<tr>
<td>Security</td>
<td>Different types of authentication devices the systems support. If the token automatically lock when to many incorrect PIN is entered, If it is possible for the administrator to unlock the token. If the token gets out of sync from the server, can the administrator re-synchronize? If the user change PIN by him self and initiate the token.</td>
</tr>
<tr>
<td>Tokens</td>
<td>Appearance of token. Battery consumption, battery life and if the batteries can be replaced by the user.</td>
</tr>
<tr>
<td>Table 7.4.5</td>
<td>Maintenance cost. Staff list for token and server licenses. Upgrade cost. Token and server license cost for 350 users. Total purchase cost for 350 users. Required hardware.</td>
</tr>
</tbody>
</table>
7.2 Examined systems

Producers of the systems that we have analysed are, according to our resellers, the most known in the world of authentication solutions. The system producers can be viewed in table 7.2.1.

For further reading, please visit their homepage.

Table 7.2.1 Producers, systems and their addresses

<table>
<thead>
<tr>
<th>Producer</th>
<th>System</th>
<th>Homepage</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActivCard</td>
<td>ActivCard AAA</td>
<td><a href="http://www.activcard.com">www.activcard.com</a></td>
</tr>
<tr>
<td>CRYPTO-Card</td>
<td>CRYPTO-Server</td>
<td><a href="http://www.cryptocard.com">www.cryptocard.com</a></td>
</tr>
<tr>
<td>RSA Security</td>
<td>SecureID5.2</td>
<td><a href="http://www.rsa.com">www.rsa.com</a></td>
</tr>
<tr>
<td>SecureComputing</td>
<td>Premier Access</td>
<td><a href="http://www.securecomputing.com">www.securecomputing.com</a></td>
</tr>
<tr>
<td>VASCO</td>
<td>VACMAN Server</td>
<td><a href="http://www.vasco.com">www.vasco.com</a></td>
</tr>
</tbody>
</table>
7.3 System overview

The systems that we have been analysing (see table 7.2.1) are very similar in the way they work. They all are based to serve VPN- and Web users that want to establish a remote connection to the company. The following part will describe how they all work, more or less, when a user are about to establish a connection to the company network and can be viewed in fig 7.3.1. This information is based on external interviews with consultants, resellers and distributors and documentation that were found at the producer’s homepage.

Figure 7.3.1 How the BTG network environment can look after the implementation.
When a remote user (1) want to establish a connection to the company’s network, they have to identify themselves with username and a unique one-time password that is generated by the hardware token (2) that are personal assigned to each remote user. This username and password are entered either on a web interface, for Web users, that are included in the system, or at the VPN-client logon window for VPN-users.

One-time password can be based on time or event, time and event synchronization or challenge-response asynchronous.

When the user has entered a username and a one-time password, a request is sent (3) to the remote authentication server via Checkpoint VPN-1 server. To minimize the risk that someone could pick up the password during the dataflow between the user and the network, an encryption algorithm is used to transform the password to an unreadable data string. This transformation is made by either 3DES or AES with a key length of 128-168 bit.

The remote authentication server (4) locates the username in the database, compares it with the password and token-code\(^3\) with its own record. If the users password combined with the token code is correct, the user is granted access. The authentication database contains information of what access rights the user is entitled to in the network.

The firewall (5) task is now to redirect the user to the right place, either to LAN (6) or DMZ (7) in this case, where another authentication has to be made.

If a user tries to access the network without the correct password, too many times, the user account will be locked down. All attempts to access the network will be logged whether they was successful or not and the log contains information like time of event and user. This is to prevent unauthorized persons to get access to the network and to detect and react to potential break-ins before they result in loss.

### 7.4 Comparison results and analysis

To be able to analyse and compare the systems, tables were set up containing the requirements and attributes from Chapter 6. Information from system documentations and consults, resellers and distributors was then noted with P (Pass) if the system supported the requirement or attribute, F (Fail) if they did not support and N/A (Not Available) if the information was not found.

All tables are followed with more detailed analyse of the most essential parts of the requirements that has to or is preferred to be fulfilled.

---

\(^3\) Token code - Every token is assigned a specific token number.
### Table 7.4.1 Description of platform, applications, VPN, and Web users.

This table describes if the systems support Windows 2000 and 2003 platform, applications like Exchange 2003, CheckPoint VPN-1, LDAP and AD.

If they can run in mixed networks like UNIX, SUN, and Novell and supports VPN and Web remote users.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Priority level</th>
<th>ActivCard AAA</th>
<th>CRYPTO Server 6.1</th>
<th>Secure ID 5.2</th>
<th>Premier Access</th>
<th>VACMAN Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2000</td>
<td>Critical</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Windows 2003</td>
<td>Critical</td>
<td>P</td>
<td>N/A</td>
<td>P</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

#### Applications:

<table>
<thead>
<tr>
<th></th>
<th>Priority level</th>
<th>ActivCard AAA</th>
<th>CRYPTO Server 6.1</th>
<th>Secure ID 5.2</th>
<th>Premier Access</th>
<th>VACMAN Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange 2003</td>
<td>Medium</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>CheckPoint VPN-1</td>
<td>Critical</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>LDAP</td>
<td>Critical</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>AD</td>
<td>Critical</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Compatibility in mixed network for TCP/IP protocol</th>
<th>Priority level</th>
<th>ActivCard AAA</th>
<th>CRYPTO Server 6.1</th>
<th>Secure ID 5.2</th>
<th>Premier Access</th>
<th>VACMAN Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
</tbody>
</table>

#### Remote users

<table>
<thead>
<tr>
<th></th>
<th>Priority level</th>
<th>ActivCard AAA</th>
<th>CRYPTO Server 6.1</th>
<th>Secure ID 5.2</th>
<th>Premier Access</th>
<th>VACMAN Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN</td>
<td>Critical</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Web</td>
<td>Critical</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
</tbody>
</table>

P=Pass  
F=Fail  
N/A=Not available

**Windows 2000 and 2003 platform**

All systems support Windows 2000 platform but only ActivCard AAA server and SecureID with ACE 5.2 server support Windows 2003. ActivCard AAA server hasn’t been certified for Windows 2003 like SecureID5.2 server, but according to Tony at Veri-sec, several tests have been made successfully. No information, at CRYPTOcards homepage, can be found whether or not CRYPTO-Server supports Windows 2003, neither can any consult or resellers confirm this. PremierAccess and VACMAN server do not support Windows 2003 for the moment.

**Microsoft Exchange 2003 Outlook Web access (OWA)**

ActivCard AAA and SecureID5.2 announce, at heir homepage, that they support Microsoft Exchange OWA, but do not specify which version it is valid for. CRYPTO-Server and PremierAccess server support Microsoft Exchange OWA 2000 server but no information is given if they supports Microsoft Exchange OWA 2003, and no reseller or consult can confirm this. No information can be found whether or not the VACMAN server supports Microsoft Exchange OWA at all.
Analysis of authentication systems
Which is the most suitable for BTG?

CheckPoint VPN-1, LDAP and AD
All systems support CheckPoint VPN-1, LDAP, AD.

VPN and Web remote users
All systems support remote VPN- and Web-users.
Table 7.4.2 Support and warranty of the systems.

This table describes if the systems support logging functions and if they are in real-time or not. With real time, we mean that the administrator can watch the logs at the same time as they occur. It also shows if the producers have support of any kind, if yes for how long time and if they provide software and token warranty.

<table>
<thead>
<tr>
<th></th>
<th>Priority level</th>
<th>ActicCard AAA</th>
<th>CRYPTO Server 6.1</th>
<th>Secure ID 5.2</th>
<th>Premier Access</th>
<th>VACMAN Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMINISTRATION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event log record</td>
<td>Critical</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>SUPPORT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System support:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td>Critical</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Time*</td>
<td>Critical</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
</tr>
<tr>
<td>National</td>
<td>Medium</td>
<td>F</td>
<td>F</td>
<td>P</td>
<td>F</td>
<td>N/A</td>
</tr>
<tr>
<td>International</td>
<td>High</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>N/A</td>
</tr>
<tr>
<td>Mail</td>
<td>Medium</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Answer time</td>
<td>Medium</td>
<td>24h</td>
<td>24h</td>
<td>24h</td>
<td>24h</td>
<td>24h</td>
</tr>
<tr>
<td>WARRANTY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td>Low</td>
<td>3 month</td>
<td>1 year</td>
<td>1 year</td>
<td>1 year</td>
<td>N/A</td>
</tr>
<tr>
<td>Tokens</td>
<td>Medium</td>
<td>**</td>
<td>5 year</td>
<td>***</td>
<td>5 year</td>
<td>N/A</td>
</tr>
</tbody>
</table>

P=Pass
F=Fail
N/A=Not available

*24 hours a day, seven days a week.

**Included in maintenance cost

***Purchased lifecycle

**Event log record**

All systems have log accessibility but they differ. ActicCard AAA-, PremierAccess- and VACMAN server uses a non real-time log function, which means that the event logs cannot be viewed at the same time as they occur. SecureID5.2 is the only one that uses a real-time function, which means that the administrator can see the events of the users at the same time as they occur, for example if the user has any problem logging in to the system the administrator can ask the users to try to logon again and follow the user by viewing the logs. No information could be found about what kind of logging function CRYPT-Server supports.

**System support**

All producers offer 24 hours telephone support and e-mail support with 24 hours answer time for users and administrators. They also offer international telephone support except for VASCO, where no information could be found at their homepage. RSA security offers both national and international telephone support.
**Warranty**

ActivCard offers only three month software warranty, but can be extended for an extra cost, the token warranty is included in the maintenance cost. All others except for VASCO where no information could be found, offers one year software warranty. RSA Security’s token warranty lasts as long as the token, this because company’s must buy the token for a specific number of months.
### Table 7.4.3 Support for authentication devices and token features.

This table describes what kind of authentication devices the systems support, if they supports token lock when to many login attempts occur. If it is possible for the administrator to unlock and re-synchronize the token. If the user can change their own token PIN and deploy their own token to the system. It also shows the design of the tokens with PIN, token battery consumption, lifetime and if it is possible for the administrator or the user to replace the battery.

<table>
<thead>
<tr>
<th>Tokens:*</th>
<th>Priority level</th>
<th>ActieCard AAA</th>
<th>CRYPTO Server 6.1</th>
<th>Secure ID 5.2</th>
<th>Premier Access</th>
<th>VACMAN Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Token (fob)</td>
<td>Low</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Hardware Token with PIN</td>
<td>High</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Hardware token for Palm</td>
<td>Low</td>
<td>P</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Token for Pocket PC</td>
<td>Low</td>
<td>P</td>
<td></td>
<td>P</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Token for Palm</td>
<td>Low</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>Software Token for Smart phone</td>
<td>Low</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>USB Token</td>
<td>Low</td>
<td>P</td>
<td>P</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart Card</td>
<td>Low</td>
<td>P</td>
<td>P</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital Certificate</td>
<td>Low</td>
<td></td>
<td></td>
<td>P</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Biometric</td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Design:** | | |
|------------|----------------|----------------|---------------|----------------|----------------|
| Key ring | Low | P | | | |
| Credit card | Low | | | | |
| Calculator style | Low | P | P | | |

| Battery: | | |
|----------|----------------|----------------|---------------|----------------|----------------|
| Consumption*** | Medium | High | Normal | High | Normal | High |
| Life (year) | Low | 8 | 3-5 | 2-5 | 5-8 | 7-10 |
| User replaceble | Medium | P | P | F | P | P |

P=Pass  
F=Fail  
N/A=Not available  
*BTG requires a token with PIN, but for future flexibility we have chosen to look at other devices.  
**Design of tokens with PIN  
***Based on, if the token uses time or event synchronization. Time synchronization has higher battery consumption.

**Token lock and unlock function**

All tokens with PIN that are supported by these systems can be locked when to many login attempts are made. This to secure that no brute force attempts can be made.

All tokens can also be unlocked by the administrator except for RSA Security tokens where no information could be found.
Analysis of authentication systems
Which is the most suitable for BTG?

Re-synchronization
All systems allow the local administrator to re-synchronize the token if that is needed, except for RSA Security tokens that have to be replaced.

Change of PIN and User self deployment
All system tokens allow users to change the PIN by themselves. To be able to change the PIN on a RSA Security token, the user self deployment tool has to be used. User self deployment tool is supported by all systems except for VACMAN server.

Token life and battery replacement
ActivCard, SecureComputing and VASCO has a token life around eight years and CRYPTOCard and RSA security has a token life time around five years. If battery replacement is necessary during this time, all token batteries can be replaced by the user or administrator except for RSA security tokens where the tokens have to be replaced.
Table 7.4.4 Authentication modes and data encryption.
This table describes if the system supports synchronous authentication mode based on event or time, or if the system supports asynchronous authentication mode (challenge-response). What kind of data encryption the system use and how long the key length is and if the systems have account locking.

<table>
<thead>
<tr>
<th>SECURITY Authentication:</th>
<th>Priority level</th>
<th>ActivCard AAA</th>
<th>CRYPTO Server 6.1</th>
<th>Secure ID 5.2</th>
<th>Premier Access</th>
<th>VACMAN Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchron</td>
<td>Time</td>
<td>Low</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>Event</td>
<td>Low</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Asynchron</td>
<td>Challenge/response:</td>
<td>Low</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Data Encryption</td>
<td>Medium</td>
<td>3DES</td>
<td>3DES</td>
<td>AES</td>
<td>3DES</td>
<td>3DES</td>
</tr>
<tr>
<td>Key-length</td>
<td>Low</td>
<td>168</td>
<td>168</td>
<td>128</td>
<td>168</td>
<td>168</td>
</tr>
<tr>
<td>Account lock</td>
<td>Critical</td>
<td>P</td>
<td>N/A</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
</tbody>
</table>

P=Pass  
F=Fail  
N/A=Not available

**Synchronous and Asynchronous authentication modes**

ActivCard AAA server uses a combination of time and event based authentication process, which means that both time and event has to be synchronized to get access. ActivCard also support challenge-response that is an asynchronous authentication mode. SecureID5.2 and VASCO use only time synchronization or challenge/response. CRYPTOCard and SecureComputing use only event synchronization.

**Data encryption**

ActiveCard AAA-, CRYPTO-, PremierAccess- and VACMAN server uses a 3DES algorithm with 168 bits long key length and SecureID5.2 server uses an AES algorithm with 128 bits key length.

**Account lock**

When it comes to account lock, it is supported by all systems except for CRYPTO-Server where no information could be found.
### Table 7.4.5 Cost analyses for the systems.

This table describes how high the maintenance cost is, if the upgrade of software is included or not in maintenance cost. Which levels the staff-list for tokens represents and cost for tokens with PIN.

Which levels the staff-list for server license represents and the cost for server licenses.

Total cost for, tokens and server license for 350 users and how many hardware servers the system require and where is should be placed.

<table>
<thead>
<tr>
<th>Cost analysis</th>
<th>Priority level</th>
<th>ActicCard AAA</th>
<th>CRYPTO Server 6.1</th>
<th>Secure ID 5.2</th>
<th>Premier Access</th>
<th>VACMAN Server</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maintenance cost/year</strong>*</td>
<td>Medium</td>
<td>~20%</td>
<td>~18%</td>
<td>~18%</td>
<td>~22%</td>
<td>~18%</td>
</tr>
<tr>
<td><strong>Upgrade cost</strong></td>
<td>Medium</td>
<td>included</td>
<td>included</td>
<td>included</td>
<td>included</td>
<td>included</td>
</tr>
<tr>
<td><strong>Tokens (with PIN)</strong>*</td>
<td>Medium</td>
<td>1-1000</td>
<td>1-9</td>
<td>5-250</td>
<td>1-249</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10-24</td>
<td>251-500</td>
<td>250-499</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>25-49</td>
<td>501-750</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>50-99</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>100-249</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>250-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cost for tokens (350 users)</strong>**</td>
<td>Medium</td>
<td>57 750</td>
<td>183 750</td>
<td>307 300</td>
<td>166 250</td>
<td>147 000</td>
</tr>
<tr>
<td><strong>Server (users limitation)</strong></td>
<td>Medium</td>
<td>25-99</td>
<td>1-9</td>
<td>1 25</td>
<td>5-149</td>
<td>1-24</td>
</tr>
<tr>
<td></td>
<td>100-499</td>
<td>100-249</td>
<td>26-50</td>
<td>150-249</td>
<td>25-49</td>
<td></td>
</tr>
<tr>
<td></td>
<td>250-499</td>
<td>50-99</td>
<td>101-150</td>
<td>100-499</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>500-500</td>
<td>100-249</td>
<td>26-50</td>
<td>150-249</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1000-251-500</td>
<td>151-250</td>
<td>500-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cost for server license (350 license)</strong></td>
<td>Medium</td>
<td>363 000</td>
<td>80 173</td>
<td>328 500</td>
<td>220 500</td>
<td>104 000</td>
</tr>
<tr>
<td><strong>Total cost</strong></td>
<td></td>
<td>420 750</td>
<td>263 923</td>
<td>635 800</td>
<td>386 750</td>
<td>251 000</td>
</tr>
<tr>
<td><strong>Extra accessories (hardware)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Servers hardware</td>
<td>Medium</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>placement (recommended)</td>
<td>Medium</td>
<td>DMZ</td>
<td>DMZ</td>
<td>DMZ</td>
<td>DMZ</td>
<td></td>
</tr>
</tbody>
</table>

*Yearly cost in percent (%) of the total cost for server license.

**Included in maintenance cost.

***Cost for tokens with PIN. (ActivCard Token, CRYPTO RB-1, RSA SD520, SecureComputing Platinum and VASCO Pro300.)

****All prices should be viewed as a guideline. Prices are in Swedish crowns and exclusive tax and comes from Danared Leif (Addsec), Börjesson Fredrik (Protect-data) and Anders Henriksson (Verisec).
Analysis of authentication systems
Which is the most suitable for BTG?

Maintenance
The maintenance cost is annual and includes the system upgrades. All producers include the first year of maintenance cost, in the server license price. The following years maintenance cost is based on the license cost.

Token and server license
All tokens are an on-time purchase, except for RSA security tokens where the tokens has a date of expire, depending on how long time the company has purchased for. The maximum lifetime for RSA security tokens are five years, and then they have to be re-purchased.

The token price is based on 350 users which BTG has to day, and as the table 7.4.5 shows there are big differences between the systems. RSA security token has the highest cost and the less expensive is the ActivCard token.

When it comes to the server license cost, it is also big differences between the systems. ActivCard has the highest cost and the less expansive is CRYPTOCard.
8 Conclusions

Our conclusion is that all the systems that we have analysed are suitable for BTG Pulp and Paper Sensors AB since they are very similar in the way they perform the authentication. The only main difference is that only two out of five of these products support Windows 2003 server, but the other will probably support this at the end of this year. But according to the requirements in Chapter 6.1 that the system had to support Windows 2003 will we not recommend these systems which are CRYPTO-Server, PremierAccess Server and VACMAN Server to BTG.

This means that it is only ActivCard AAA server from ActivCard and SecureID5.2 form RSA Security that are suitable for according to the requirements that are set by cooperation with BTG.

We have chosen to recommend ActivCard AAA server, since the purpose of this report is to recommend one suitable system.

The ActivCard AAA server’s advantages compared to the SecureID5.2 server is that the token can be re-synchronized by the administrator if that is needed, this is not possible with RSA Security tokens that has to be replaced.

Another advantage is also the use of a strong authentication technology since it combines the time and event synchronization. This means that both the time and the event counter has to be synchronized with the token to be able to access the company network. This functionality is not supported of any of the other analysed systems. ActivCard token has longer lifetime, about eight years, compared to RSA Security tokens that only has a life time of maximum five years and then have to be repurchased.

Another advantage that ActivCard has compared to RSA Security is that it is less expensive.

The only disadvantage ActivCard has compared to RSA Security it that they do not support national telephone support.
References


Buss Tony. Technician. Verisec. Telephone and e-mail communication. 2004-05-13

Börjesson Fredrik. Technician. Protect-Data. Telephone and e-mail communication 2004-05-13

Danared Leif. Salesman. Addsec Telephone and e-mail communication 2004-05-13


Larsson-Steen Tord, Supervisor, BTG, Säffle, meeting 2004-03-19

Lindmark Johan, BTG, Säffle, meeting, 2004-03-19


Analysis of authentication systems
Which is the most suitable for BTG?

Unicenteradvisor
http://www.unicenteradvisor.com/doc/05184
2004-04-27

Vasco, Whitepaper
2004-04-20

Vasco, authentication whitepaper
2004-04-20

Whatis
http://www.whatis.com
2004-04-15

Yourencyclopedia, qualitative method
http://www.yourencyclopedia.net/Qualitative_method.html
2004-05-16

Other references

These are references that have indirectly affected our analyse, but are not specified in the report.

ActivCard
http://www.activcard.com
2004-05-05

Check Point, VPN-1 Client
http://www.checkpoint.com/products/connect/vpn-1_clients.html
2004-04-15

CRYPTOCARD
http://cryptocard.com
2004-05-05
Telephone and e-mail communication. 2004-05-13

HowStuffWorks, How Virtual Private Network Work
By: Jeff Tyson.
http://www.howstuffworks.com/vpn.htm
2004-04-15
Analysis of authentication systems
Which is the most suitable for BTG?

RSA security
http://www.rsa.com
2004-05-05

SecureComputing
http://securecomputing.com
2004-05-05

VASCO
http://vasco.com
2004-05-05
Analysis of authentication systems

Which is the most suitable for BTG?