Product Data Technology in a network:

White Paper for PDTnet Authorization and Security Concepts
## History

<table>
<thead>
<tr>
<th>Version</th>
<th>Status</th>
<th>Authors</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0</td>
<td>Draft</td>
<td>Oliver Guntermann, PROSTEP</td>
<td>Creation</td>
</tr>
<tr>
<td>0.1</td>
<td>Draft</td>
<td>Oliver Guntermann, PROSTEP</td>
<td>Results from July Workshop</td>
</tr>
<tr>
<td>0.9</td>
<td>Draft</td>
<td>Oliver Guntermann, PROSTEP, Olaf Kapinski, PROSTEP</td>
<td>Network security</td>
</tr>
<tr>
<td>1.0</td>
<td>Final</td>
<td>Oliver Guntermann, PROSTEP</td>
<td>Implementation Example</td>
</tr>
</tbody>
</table>
Contents

PREAMBLE .................................................................................................................. 4
1 BACKGROUND AND MOTIVATION ....................................................................... 5
2 GENERAL SCOPE ................................................................................................... 6
3 NETWORK SECURITY .............................................................................................. 7
  3.1.1 Communication between Client and Front end server (1. Tier) ...................... 7
  3.1.2 Communication between Server and PDM system (2. Tier) ......................... 9
  3.1.3 Possible Attack Scenarios ........................................................................... 10
4 DATA ACCESS ......................................................................................................... 12
  4.1 User, Development Project and Role ............................................................... 13
  4.2 Access rights ..................................................................................................... 13
  4.3 Use cases and Access Rights ............................................................................ 13
    4.3.1 Start node identification ........................................................................... 13
    4.3.2 Browsing down ........................................................................................ 14
    4.3.3 Browsing up ................................................................................................ 15
    4.3.4 Download of files ...................................................................................... 16
    4.3.5 Upload of files .......................................................................................... 16
    4.3.6 Upload of metadata including structures .................................................... 16
    4.3.7 Search in design space .............................................................................. 17
5 SAMPLE IMPLEMENTATION .................................................................................. 18
6 SUMMARY ............................................................................................................... 20
PREAMBLE

This document is a versioned document containing requirements and results of the PDTnet project. Due to its character of a „living document“ it will be extended and completed gradually according to the progress of the PDTnet project. This is why not all chapters will be completely finished in this document version.
Third parties are kindly invited to provide their comments and additional requirements to the PDTnet project (pdtnet-contact@prostep.de).
1 BACKGROUND AND MOTIVATION

The PDTnet project will give user outside a company network access to data inside the companies PDM system. This process involves a lot of security issues. The access to the PDM system has to be secured, so that only authorized users can login into the system, the transport from and to the system has to be secured so that third parties can not read the data and the users should only access data they are allowed to see.

A PDTnet scenario can only be successful if these three assumptions are valid. During the design of a PDTnet system the data security is a crucial part of the implementation.

This paper can only give an overview over the topics in connection with security. It is not intended to be a complete guide to a secure system. Its goal is to give an overview about the involved topics. All implementation details depend on the scenario, the transport mechanisms and the used PDM system and are heavily scenario dependent.
2 **GENERAL SCOPE**

This paper covers two different layers regarding security and access to product data. The first layer covers network access and transportation of product data over worldwide networks. The second layer describes general mechanisms for administration of access rights inside of a PDM-System. The following picture gives an overview of the two layers:

The first layer will be covered by the network security chapter, the second one by the data access chapter.
3 NETWORK SECURITY

The scenario covered by this chapter is access from a PDTnet client over a network on a PDTnet server which serves as a front end to a PDM system. The following graphic describes this scenario and is divided into three tiers.

The first tier is the connection between the PDTnet client and server which needs to be secured. The second tier is then the access from the PDTnet server to the PDM system. The third tier is of no interest for this paper as the connection between the PDM system and its database is considered as already secured by the system vendor.

3.1.1 COMMUNICATION BETWEEN CLIENT AND FRONT END SERVER (1. TIER)

There are two aspects to consider for this tier:

- Secure transport of data (passwords are also just data from a transport point of view)
- Prevent unauthorized access to the front end server

The PDTnet scenario supports two different kinds of transport mechanisms, over the internet or the much more secure ENX network. The difference between both networks is that ENX is a closed network where not everyone gets access to.
The ENX scenario is identical to the internet scenario, only the transport mechanism is different.

The (physical) network tier is transparent for the client and the PDTnet server. To enhance security a https tunnel is used on top of the network. After the exchange of the encryption keys the data transport is encrypted and can be considered secure.

The certificates the server sends guarantees that the client is connected to an authorized server. This prevents a possible server spoofing (or man in the middle attack), where an attacker intercepts the communication and acts as the server against the client side and as the client against the server side. All communication after the key exchange is encrypted and not decrypt able from 3. persons (when using actual encryption key length). The user authentication runs in the encrypted tunnel, so the password can not be read by third parties. The mechanisms behind a https tunnel make it impossible to hijack an established session because of the public/private key system.
3.1.2 COMMUNICATION BETWEEN SERVER AND PDM SYSTEM (2. TIER)

Attacks against this level are much more complicated. An attack is only possible if the attacker has access to a computer in the DMZ. Then he can listen to the unencrypted back end communication (either CORBA or http).

To prevent this kind attacks it is necessary to increase the security on all computers in the DMZ. Standard mechanisms for hardening computers against should be used on all machines. This includes:

- Remove all unnecessary services
- Use encrypted (secure) versions for standard protocols (i.e. ssh instead of telnet)
• Remove all unnecessary users from the computers
• Protect the computers via firewalls
• Use intrusion detection systems
• Use oversized machines to prevent denial of service attacks

3.1.3 **POSSIBLE ATTACK SCENARIOS**

3.1.3.1 **Attacks against the client**

There are different scenarios how an attacker could directly attacking the client or the session on the client machine:

- keyboard logger, screen dumper etc. ("Trojan Horses")
- direct attack to get the private key and hijack the session after user authentication (not known yet)
- brute force methods to try all passwords

Also there is a number of possible indirect attacks against the passwords, mostly due to the choice of insecure passwords:

- search for plaintext saved passwords ("passwords.txt")
- "social reengineering" of user-selected passwords ("name of children etc.)
- ask for a password ("I forgot mine...")

The first group of attacks can be preventing by enhancing the security of the client computers and the choice of long passwords so that brute force encoding needs very long time. The second kind of attacks can only be prevented by instructing the users about security topics.

3.1.3.2 **Attacks against the server**

If an attacker wants to attack the server he needs to hack the front end server through the firewall. Typical scenarios are:

- use errors in the system (OS or applications) to infiltrate malicious code
- crash the machine because of overload (dDOS, distributed denial of service)

To protect the computer make it as simple as possible. Run only the absolutely needed number of services. Oversize the firewall computer to prevent dDOS attacks.

3.1.3.3 **Attacks against the 1. tier communication**

This is the classic "man in the middle" attack. Another computer intercepts the communication between client and server and reads all data send. A possible scenario would be:

- use ARP-Spoofing to redirect traffic to attackers machine
- relay machine sends own certificate and connects to front end server
- user gets the message: "certificate changed"
- the relay machine spies all traffic in https tunnel
This attack can be noticed on the client side because of the certificate changed message, which must be affirmed by the user. Again a minimum of user instruction can prevent such an attack.

3.1.3.4 Attacks against the 2. tier communication

This is an indirect attack against the PDTnet computers. The attacker uses another computer in the DMZ which is less protected to listen to the unencrypted data transfer between the PDTnet front end server and the PDM system. It is only possible:

- If the attacker is a valid user in the DMZ or
- If he can get access to a less secured server in the DMZ

To prevent such an attack all servers in the DMZ must be secured as good as possible.
### 4 DATA ACCESS

After a user gets access to a PDM system it must be decided, which objects in the system he can view, download, modify etc. The different kinds of access a user may have depend on the development project and the role the user has in this project. For every object a decision has to be made which access is granted.

The goal of this chapter is to describe how

- to limit access of user to product data in his scope
- to give authorized users access to all data they need for their work
- to supply a robust set of rules to start with
- to reduce administration overhead

These goals lead to a conflict between security, necessary access to product data and administrative overhead.

Giving users to less access leads to unnecessary stops in the construction process and as consequence to delays. To much access can have severe consequences if information gets into wrong hands. And a decision entry by entry needs a lot of administration which nobody can provide.

This chapter gives some guidelines how to limit access of partners to the product data they are allowed to read. These guidelines only cover the scope of the current use cases. New use cases or extensions of the current use cases may need changes also in this document.

The first chapter will give an overview about the relation between user, development project and role to access rights. In the chapter 4.2 the needed access rights are discussed. The next chapter will discuss the different use case scenarios, which rights are necessary for them and propose a set of default rules.
4.1 USER, DEVELOPMENT PROJECT AND ROLE

A development project contains all objects (PDM data, documents, etc.) needed for construction purpose. Different users will have access to the development project and work together in the design process. Users can be internal users (access rights of this group is handled by a corporate process and not topic of this document) and external users. The access of external users must be handled very carefully and should be limited to the absolute necessary minimum. For example no external user should get administration privileges, external users should not be able to read, data which was given free for them, etc.. To restrict the rights of external users a special role can be created (for example 'external user') and the access rights of this role are very restricted. The role defines a kind of template for the access rights of all external users.

4.2 ACCESS RIGHTS

Different PDM system have their own set of ‘native’ access rights. This document will use a limited set of ‘neutral’ access right, which are sufficient for the current use case. These access rights can be mapped more or less directly to the ‘native’ access rights. New use cases may need to extend the set of these rights.

<table>
<thead>
<tr>
<th>Access right</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td>read of original data (structure, metadata)</td>
</tr>
<tr>
<td>View</td>
<td>simplified or read only content of digital files, View includes Read and may need additional processes, for example automatic generation of simplified cad models (currently not covered)</td>
</tr>
<tr>
<td>Download</td>
<td>download of digital file/metadata, this includes Read and View</td>
</tr>
<tr>
<td>Write</td>
<td>change PDM meta data (currently not covered by the implemented use cases)</td>
</tr>
<tr>
<td>Create</td>
<td>create a new object in the PDM system</td>
</tr>
<tr>
<td>Upload</td>
<td>upload a new version of a document, this is either a Write or a Create/Write but may also involve other workflow processes like document versioning etc.</td>
</tr>
<tr>
<td>Search in design space</td>
<td>this access right differs from the above as it is a right of a user and not attached to an object in the PDM system</td>
</tr>
</tbody>
</table>

With the exception of ‘search in design space’ all these rights grant a different kind of access to specific information stored in the PDM system. The ‘search in design space’ access right is different as it gives the user access to a process which may show him the existence of objects he has no access to. In this case only the existence is flagged, but no other access is given to the nodes.

4.3 USE CASES AND ACCESS RIGHTS

The following chapters will discuss the current use cases and which access rights are involved.

4.3.1 START NODE IDENTIFICATION

The PDTnet browsing process starts from a set of nodes, the start nodes. A user needs a part number or name and the version to select the root node for his view on the product tree. He may only select nodes which are set as start nodes for him.
As the next screen shot shows, the user needs **read** access to the part number and name of a start node.

### Process:

Assigning a node as start node for a user includes granting **read** access to the basic information of a node, the part number and part name.

#### 4.3.2 **BROWSING DOWN**

Show the children of the selected node and additional information (metadata) about the browsed node. In the PDTnet browser this is done by two different access requests, the first for the basic information like part number and name and an additional request if the user wants to access the meta data.

For both requests the user needs **read** access to the according data. In the case of browsing it is access to the basic information like part name and part number, in the metadata requests it is **read** access to the metadata.

The next screen shot shows an example for a browsing down request.
Granting these rights also involves giving the same access to the children, grandchildren etc., it is a recursive process. This access should not be extended to documents, viewing of documents is another use case and should be handled separately.

Normally a user should be able to do a browsing down from his start nodes.

### 4.3.3 BROWSING UP

The browsing up use case covers to different scenarios. The first is to show the parent node of the current one, the other is to show the root nodes of all product trees the current node is element of.

The access rights involved are the same as in the browsing down case, the user needs at minimum access to the basic information and may also be granted read access to the PDM metadata.

**Process:**

Access to nodes upwards of the start node has to be given explicitly. The process should not give access to any other node like in the browsing down case. If the user
needs access to a lot of nodes upwards from the start node a higher start node should be chosen.

4.3.4 **DOWNLOAD OF FILES**

This use case covers the transfer of metadata or document files from the PDM system to the local system. The access to the metadata is identical to the normal read on metadata, no extra download right need to be granted as a user can simply copy and paste the information from the browser. For the download of documents a specific download right has to be granted.

Process:

By default user may only download documents he owns, no download right is given to other documents. The right to download other document must be given explicitly and Document by document.

4.3.5 **UPLOAD OF FILES**

The upload of files use case describes the transfer of local files to the PDM system. Like the download case this may be metadata or documents. To be able to upload files the user first needs read access to navigate from a start node to the node he wants to upload data. Then he needs write access to the metadata or upload access to the document files. The upload of document files is handled differently as this case also involves other processes like versioning etc.

Process:

By default, no upload access is given and must be granted separately for every metadata or document entry. If a user uploads a file he gets automatically download and upload access to the new version.

4.3.6 **UPLOAD OF METADATA INCLUDING STRUCTURES**

The upload of metadata including structures is identical to the already existing offline data exchange. In the most cases this includes complex workflow, for example assigning of valid part numbers. For this kind of data exchange the user needs right identical to the upload of files and also the right to create new nodes in the product tree.

Process:

A user who uploads data in this use case gets automatically read access to all new nodes and metadata and download and upload access to the transferred documents. Other users should get read access to the basic information and or metadata of new nodes according to the access right they have on the start node of the transferred structure but no access to new created document files.
4.3.7 SEARCH IN DESIGN SPACE

In this use case the user searches for all nodes in a given geometrical design space. The involved search in design space access right differs from the other rights as it is not given to a node but a user. In the case of a search in design space the user needs also information about nodes he has no read access to (a flag that there are nodes he has no access to, so that he can ask for access). If such nodes are not ‘flagged’ a designed part may not fit in the design space later because it conflicts with other parts the user had no access to.

Process:

The search in design space right depends on the role the user has in a development project and not from a node. All nodes the user has read access are shown in a tree, the nodes he has no access to are ‘flagged’.
5 SAMPLE IMPLEMENTATION

This chapter describes a sample implementation for of the above described schema on the PDTnet demo server.

The demo server uses IMAN as the underlying PDM-system. To implement the access rights, IMAN allows a fine granular schema via a rule tree. A new role (supplier) is added and contains the rules for the PDTnet access scenarios.

The goal of this implementation is to give suppliers access to

- their own objects (read and write)
- the objects which are free for public access to all suppliers in iMAN
- the objects which are released for common supplier access by the OEM or by the supplier who is the owner of the object (read only)
- the objects which are released for the special access of a certain supplier by the OEM (read and write)
- the objects which are released for all participants of a certain project by a supplier (read only)

The implementation can be tested on the PDTnet demo server. The server contains two projects and four users with different access scopes. One of the user is the OEM, the three other users are suppliers working for one of the two projects.

<table>
<thead>
<tr>
<th>User</th>
<th>Password</th>
<th>Access to</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>oemuser1</td>
<td>oemuser1</td>
<td>project1 and project2</td>
<td>designer</td>
</tr>
<tr>
<td>supplier1</td>
<td>supplier1</td>
<td>project1</td>
<td>supplier</td>
</tr>
<tr>
<td>supplier2</td>
<td>supplier2</td>
<td>project1</td>
<td>supplier</td>
</tr>
<tr>
<td>supplier3</td>
<td>supplier3</td>
<td>project2</td>
<td>supplier</td>
</tr>
</tbody>
</table>

The main rule for defining access is the item type. External users only get access to items of the type foreign part. All other items are not accessible for users which have the role supplier.

The decision which kind of access (in the demo server only read and write are implemented) is based on the status of the item. In our simple scenario three different states are implemented:

- working: not a real status type, all objects which do not own a status are in ‘status’ working. ‘Working’ foreign parts are accessible only for their owners and for project members.
- supplier private: The objects are only accessible for the owner
- supplier project: Those objects are accessible for reading for all suppliers in a certain project
- supplier public: Those objects are accessible for reading for all suppliers

Of course a ‘real’ PDTnet server would need some more states but for our demonstration these three status types are sufficient.
The IMAN Rule Tree Methods used for access control are very simple:

- has type ‘foreign part’
- has status ‘supplier private’
- has status ‘supplier project’
- has status ‘supplier public’

IMAN uses access control lists to connect the decisions with the above defined methods. The entries in this lists define which access is allowed for a specific item based on its status type. These access rights must be defined for:

- the owning user
- users with role ‘supplier’
- users with role ‘designer’
- all other users (world)

The following pictures shows a part of the Iman rule tree used for the demo server:
6 SUMMARY

Setting up a secure environment to allow users outside of the company access to PDM data is a complex task which should not be underestimated. It involves two different levels of security to be carefully planned:

- The access to the front end server
- The access to the data stored in the PDM system

This document can only give some hints for the design of a secure PDTnet system. It cannot be a complete guide for security! All necessary tasks are scenario dependent and design decisions have to be made for every specific case.