

## **1.1 Manufacturing Enterprise Security**

In the area of manufacturing the protection of technical data (e.g. construction plans, simulation results) is of outmost importance for the commercial success of a company, since quite a huge amount of manpower and expertise has to be invested into the creation of these data and these documents contain a lot of valuable information about future products or plans. Besides technical data as CAD models and VR data this applies also to other non technical, business related documents (e.g. strategy papers, business plans, schedules, minutes of executive meetings, internal progress reports, proposals). Thus an intelligent manufacturing environment must not only provide innovative approaches to generate and work with data, but must also protect them.

Nowadays access to the global network has become a necessity and almost all the company networks have become interconnected and closely interwoven. However, with the provision of the technical means for legitimate users to access sensitive information located inside a company network from the outside one loses a line of defence against illegitimate users. It becomes much harder to control the access to the intranet.

Hand in hand with the fast evolution of the cooperation technologies (networking) one can observe an increasing amount of close cooperation on an organizational level. As reaction to the challenges of the global market, companies form alliances and cooperate in particular areas. For the partners it is essential to exchange sensible information with their respective partners. These alliances will change over time and each of the partners in such an alliance can be involved in further alliances. The task of exchanging confidential data with some partners but ensuring at the same time that no illegitimate users can access this data is quite a hard one, since it requires trust in and cooperation from the partners.

The technical development in the area storage devices (miniaturization, USB Tokens), mobile computers (Laptops, PDA) and ad-hoc networking (e.g. IEEE 1394 Firewire, USB, ...) brought considerable changes and improvements in the working style. As a result, it has become very easy to transfer huge amounts of data between different devices and many of these devices can easily be carried around (USB memory sticks, PDAs, cellular phones). However, when providing these technologies (ad-hoc connectivity and small size) for the benefit of legitimate users, they are also available for illicit usage (e.g. data theft or industrial espionage), since currently an access control mechanism is lacking which is fine grained enough to distinguish between legal actions and illegal ones. For example in the IEEE 1394 standard (Firewire) it was possible to read out the entire content of a computer's hard disk circumventing the operating system and any access restrictions it tries to establish.

Thus, IMS will provide as an integral part of its basic service infrastructure on (Technology Layer, see **Error! Reference source not found.** on page **Error! Bookmark not defined.**) a security solutions, which can also cope with the challenges posed by recent developments:

### **1.1.1 Objectives**

The goal of the Manufacturing Enterprise Team can be formulated as "Protect sensitive data in Interconnected Environments". Therefore it will develop several solutions which allow a company to monitor and control the flow of its sensitive data in such an interconnected workspace. With these solutions companies can define and enforce (security) policies to protect their intellectual properties and ensure confidentiality of manufacturing data. In a manufacturing environment it is required to support heterogeneous platform. Thus IMS will develop security mechanisms in a system-independent manner and allow enforcing such security policies consistently on several general purpose operating systems, particularly the

Windows NT family of operating systems (including Windows 2000, XP, and 2003), as well as Unix derivatives.

To succeed in such a heterogeneous environment based on commercial off-the-shelf (COTS) systems, any policy enforcement mechanism must generally be completely orthogonal to existing mechanisms and must not affect application programs and users operating within the limits of a given (set of) security policies.

The operational basis is formed by the concept of an externally controlled reference monitor (enforcement modules) embedded in the operating system (ideally in a trusted subsystem) alongside with instrumentation; which is necessary for collecting information from the operating system components not available to existing security mechanisms as well as for enforcing security policies in the instrumentation mechanisms.

IMS will develop several components to secure the different channel, via which data can be exchanged and leaked. Each of these components can be used as standalone solution. However the best protection can be achieved by combining the various components. Thus IMS will also work on integrating all the components into one overall security solution.

As a result, corporations and governments can define security policies once and enforce these consistently throughout the organization while retaining the investments made in equipment, software, and user training (including existing heterogeneous environments) since legitimate application and user behavior is not affected.

IMS will develop security mechanisms, which can be part of an integrated solution or be used as standalone solution for the following areas.

- **File system Security:** Protect any kind of sensitive data, which is stored in the file system and ensure that only legitimate user have access to sensitive data.
- **Device Interface Security:** Enable the fine-grained control over data exchanged via and with the device interface.
- **CAD&VR Data security:** Research and provide solutions based on 3D-watermarking for 3D data

Besides the work on the individual components<sup>1</sup>, IMS also works on an integrated solution. This solution ought to realize a **secure engineering work station**. The idea is not only to combine the different individual solutions but also gain some more security by having the different components work as a collective. This brings the following benefits:

- As soon as one of the components detects a threat, also the other components, which would not be aware of the threat, can be informed about it and can take a proper action.
- By sharing and combining the information from the different security components, one can draw better conclusions on what the user is about to do, and whether this action is in line with the security policy.
- Policy rules can be specified on higher abstraction level.

Common objectives for all the security solutions are:

---

<sup>1</sup> The original development plan did not include the component for the CAD & VR data security, instead it was planned to also develop a security component for the network and central component to coordinate the different components. This coordinating component should use a new innovative, way to represent policy-rules based on using formal logic. At the end of the first year it has been recommended to the IMS project by the reviewer to focus on the security of 3D construction data. In order to allocate the required man power for this new goal the work on the network component and the central coordination component had to be cancelled.

- Security mechanisms must be applicable for in heterogeneous environments (Windows NT family and Unix derivatives)
- Security mechanisms must be transparent to applications, i.e. compatible to COTS (commercial, off-the-shelf) and customer specific applications. For a corporation it is essential, that the security solution does not restrict the usage of software.
- A system administrator must be able to configure the components according to the security policy of the company. The configuration of a large number of work stations should be possible in an effective way.
- A user<sup>2</sup> must not be able to circumvent the security solutions
- The security solutions must be as transparent as possible to the user. As long as the actions of the user are in accordance with the security policy the system should behave identical independent of whether or not the security mechanisms is installed or not.

### 1.1.2 State of the Art

Current COTS operating systems or add-on elements are unsuitable to counter threats found in modern, internetworked environments required for the productive use of advanced information systems and communication technology.

*File System Encryption:* While file system encryption mechanisms exist, these suffer from a number of limitations. Most operate only on specific file systems (e.g. Microsoft EFS) or require container volumes (e.g. McAfee PGPDisk); typically these also do not offer granularity at the individual file level for controls.

*Interface Protection:* There exists no built-in mechanism for device interface and PnP protection in COTS operating systems; some products (e.g. DeviceLock by SmartLine, Inc; Sanctuary Device Control by SecureWave DeviceWatch; DeviceWatch by ITWatch) offer limited protection at coarse granularity in both the level of control over devices and protocols and time resolution.

*Mail security:* Existing mail security products suffer from a number of weaknesses, including usability, vulnerability to Trojan horses, or in case of central mail security solutions, a single point of failure attracts attackers.

*Process Isolation:* There exists no process isolation mechanism for COTS operating systems; earlier research systems such as the U.S. National Security Agency's DTM provided simple instances of such mechanisms although this system was incompatible with COTS application programs.

A number of government agencies (e.g. Bundesamt für Sicherheit in der Informationstechnik, Germany; National Security Agency, USA) have also started working on hardening existing systems and permitting interoperability between existing systems and applications (e.g. the DTM and SELinux projects at the U.S. NSA, the SINA projects at the German BSI; ongoing transformation efforts by the U.S. NSA Information Assurance Directorate); at the same time large ISVs (e.g. Microsoft Corp.) are beginning to re-orient their security systems, putting the research discussed here at the forefront of development (e.g. the Microsoft NGSCB and TCG efforts).

There are ongoing IEEE standardization activities in the area of operating system security (P2200) and storage security (P1619) where various government and defense agencies as well as civilian entities collaborate; a member of IGD is vice chair of the sponsoring IEEE task force and actively participates in these working groups.

---

<sup>2</sup> I.e. a user without administrative privileges.

*Secure operating systems:* Primarily United States government (National Security Agency) for internal use (e.g. Trusted Mach, DTM) and commercial vendors adapting to U.S. government requirements (e.g. Sun Trusted Solaris). These systems do not support standard application program interfaces and applications.

*File System Security:* Several research prototypes as well as products by specialized small vendors (e.g. SeNTry 2020 by Soft Winter) exist for various platforms that typically operate at the volume level; a simple implementation for the Microsoft Windows 2000/XP environment is provided by Microsoft EFS, which is limited to a single file system type.

*Device Security:* Some products offering elements of required protective measures exist, e.g. DeviceLock by SmartLine, Inc; Sanctuary Device Control by SecureWave DeviceWatch; DeviceWatch by ITWatch. These, however, are restricted to a rather coarse granularity in both the level of control over devices and protocols and time resolution.

*Watermarking:* While for other types of media (e.g. audio and still images) watermarking technology has become state of the art (SysCop) and is also available in the market (MediaSec/Thompson, DigiMark, MarkAny). Watermarking for 3D data is quite a new area. Fraunhofer IGD is one of the leading institutions doing research in the area of watermarking of 3D data and it has applied for a patent for its technology.

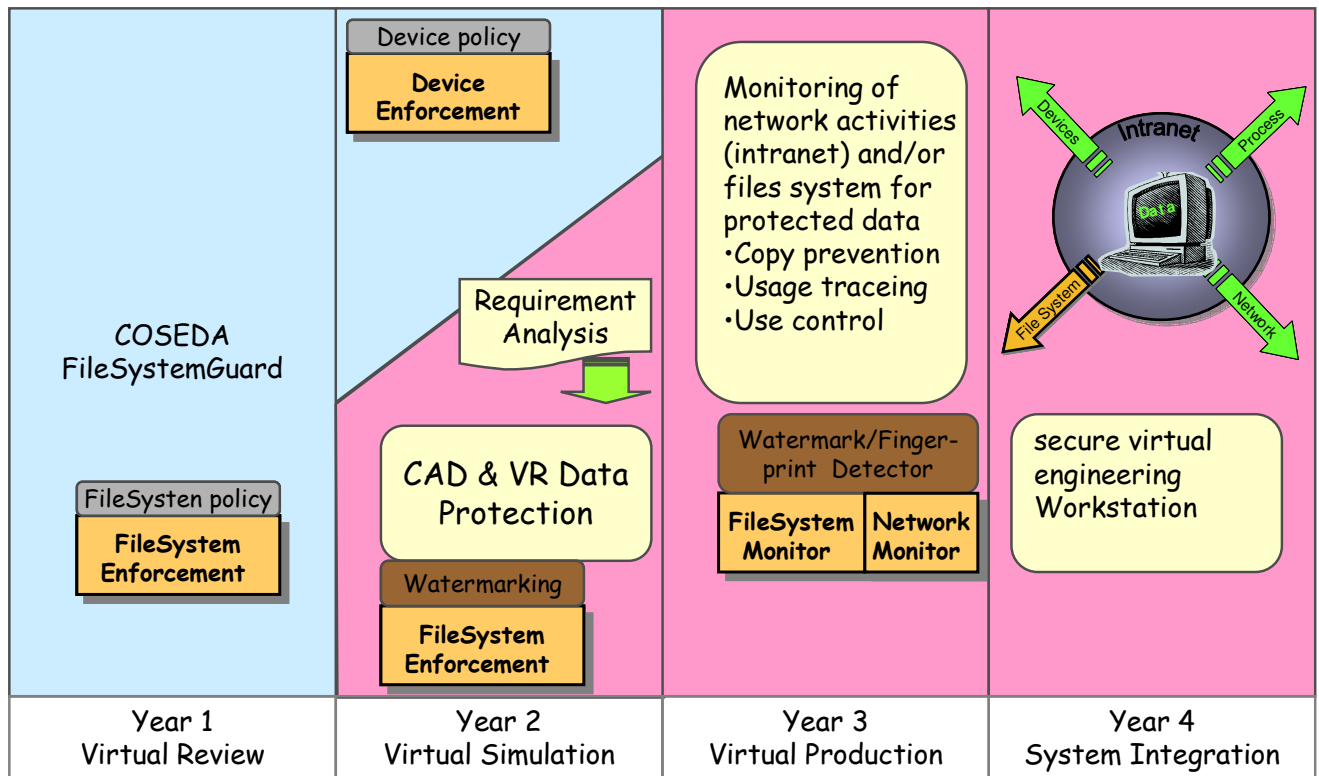
### **1.1.3 Expected Outcome**

For the application area manufacturing it is crucial, that the security mechanisms to be developed can transparently be used together with any arbitrary software used as part of the manufacturing process. Also one has to consider the issue of user acceptance. A good security mechanism shall impose as little additional effort to the user, but the user must not be able to circumvent the security mechanisms. As a consequence of this the security services will be realized as operating system extensions.

Windows 2000/XP has been chosen as the implementation platform the IMS project, since this is the operating system most relevant to the market. Based on the feedback for the first year's review the development plan for the MES team has been changed. Figure 1 below shows the revised work plan.

### **Overall planning**

The work plan of the MES team has been revised and changed from its original form. This section will give an overview of the two lines of development and how the new plan fits together. Figure 1 shows how the original line of development (COSEDA) is merged into the new line of development (3D watermarking).



**Figure 1: Overview development plan (Revised version)**

As originally planned, FileSystemGuard has been delivered in the first year. In the second year DeviceGuard has been delivered; however, only in reduced form. The support for the central security policy module without the support for originally planned central security-policy module (SPM). Since the reviewers at the end of the first project year suggested revising the development plan to also address the issue of 3D CAD data, a requirement analysis has been performed among the IMS industry contacts. Based on this requirement analysis it was decided to implement a security framework using Watermarking technology (3DGuard). It is planned to implement during the second half of the second research year to implement the basic watermarking framework, and spend the 3<sup>rd</sup> year with the research and the implementation of the various applications for 3D watermarking. In the fourth research year the outcomes of the first three years are combined into an integrated system and implement a synchronization layer to achieve additional benefits from the combination of the three individual solutions.

In the rest of this section, the different products to be developed in the IMS project will be described in more details. The product names used in this document are only used project internal ones. Finding official product names and making sure that these official names do not violate trademarks is part of the commercialization activities.

Product	Availability	Description
FileSystemGuard	End of year 1	Security solution for protection of data stored in the file system in a heterogeneous environment. This solution will automatically ensure that data stored in the file system is always encrypted. The encryption and decryption of the data is implemented in a way that it is totally transparent to the user/application. The encryption mechanism respects the file system semantic, thus system tools, as e.g. backup software, can treat them as normal files.
DeviceGuard	End of year 2	Security solution allowing the fine grained control over the data exchange with devices. This solution integrates itself into the device management routines of the host operating system. There it

		will monitor all ongoing activities and prevent any activities which are not explicitly allowed by the administrator. Thus, a system administrator can restrict the usage of devices, amongst others, to certain trusted users or devices.
3DGuard	End of year 3	<p>Security solution to automatically embed watermarks into and 3D CAD data and detect them. Using watermarking technology allows to strongly associate/embed additional data with the original data (a 3D model).</p> <p>This additional data can be used for quite a few purposes:</p> <ul style="list-style-type: none"> <li>• Copyright Protection</li> <li>• Monitoring of usage</li> <li>• Access control</li> <li>• Payment and Billing</li> <li>• Document Management</li> </ul> <p>3DGuard consists of a framework for the automatic recognition of watermarked and watermark able documents and all the basic services for document management and embedding and removal of watermarks. The actions of this underlying framework are controlled by exchangeable security policy components. The different security policy components realize the different application areas for the watermarking</p>
Secure engineering work station	End of year 4	Combination of FileSystemGuard, DeviceGuard and 3DGuard into one integrated solution with additional coordination layer for the synchronization of the individual components

**Table 1: Marketable outcomes from the MES team**

## **FileSystemGuard**

In the first year the enforcement modules for the file system security shall be developed. These enforcement modules will monitor all significant events and operations taking place in the file system, transforms them to a platform independent abstraction level, submit these notification to a trustworthy component for checking whether these events and actions are in accordance with a given security policy and if necessary take steps to enforce compliance with this policy. Besides preventing illicit operations from taking place these enforcement modules will offer the functionality of transparent en- and decryption of all data with standard, state of the art ciphers (e.g. AES or 3DES).

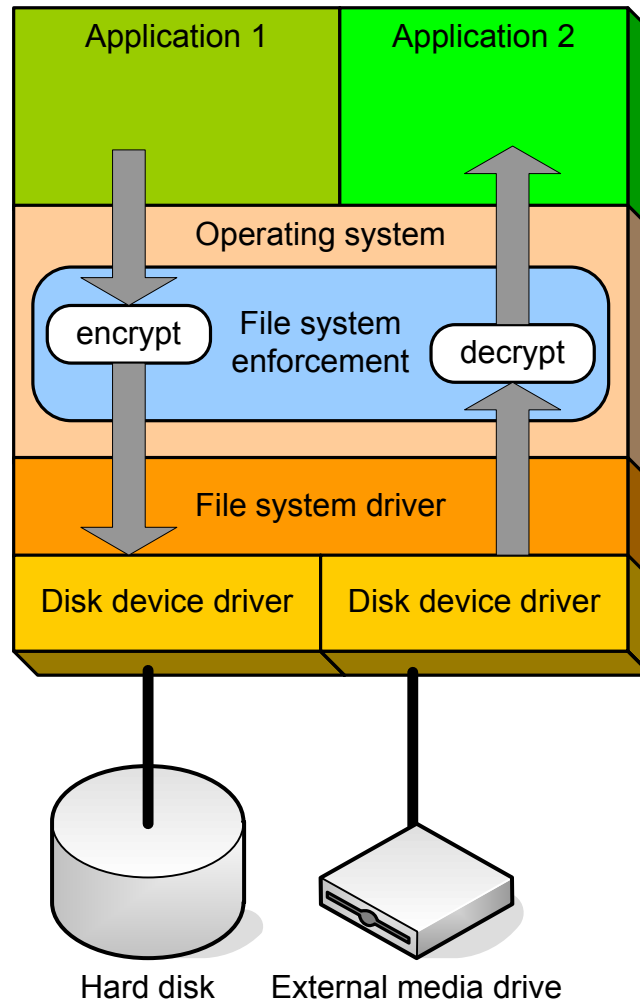
The file system enforcement modules together with this controlling security policy component will be released as the FileSystemGuard product.

The FileSystemGuard product shall provide

- system authentication
- user authentication,
- local file system encryption
- remote file system encryption

The encryption scheme used shall realise

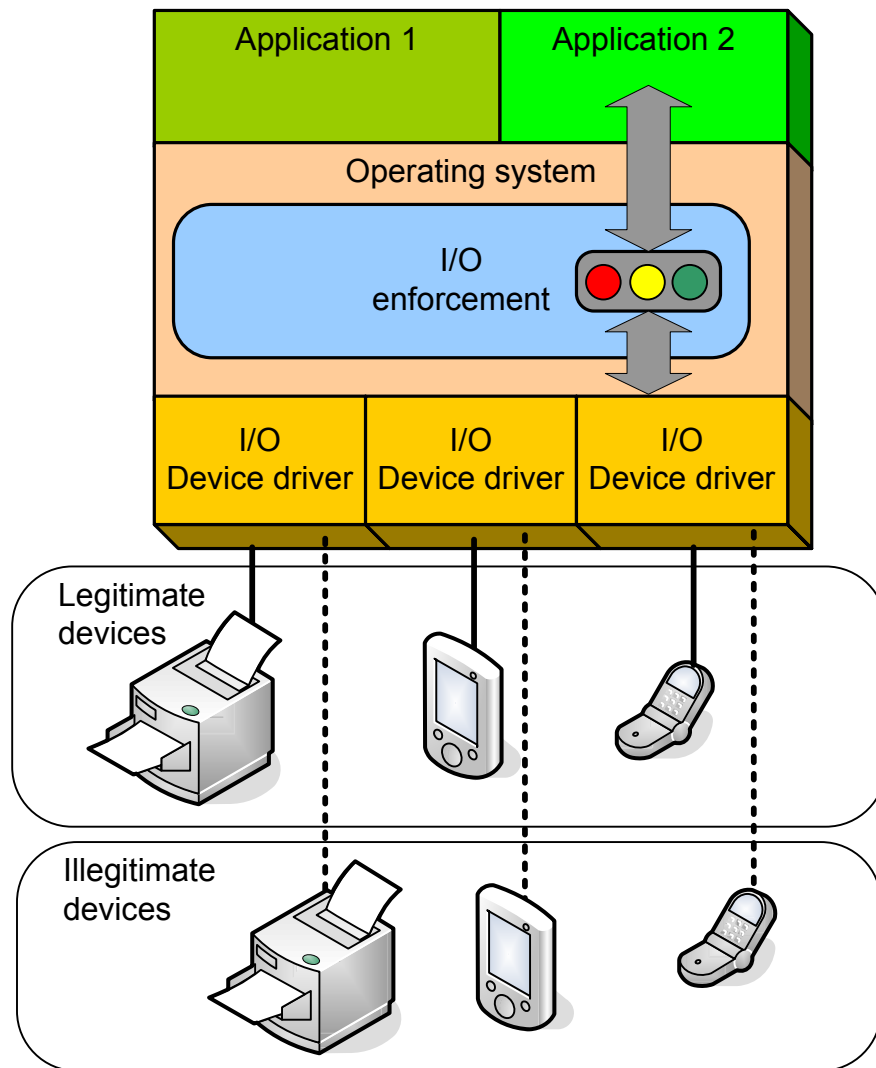
- system- and user-specific file system encryption
- separation of multiple users
- encryption mechanism is transparent to users
- file system independent encryption
- transparency to applications,
- interoperability with other operating systems



**Figure 2: System architecture FileSystemGuard**

## DeviceGuard

In the second year the enforcement module for interface security are developed. These enforcement components will monitor the activities at the workstation's device interfaces to detect and block illicit activities. In order to become a full featured product these enforcement components must be supplemented by a device interface security policy component. The complete product, which shall be named DeviceGuard, will provide the functionality to analyze, to record and to control data streams to and from individual devices.



**Figure 3: System architecture DeviceGuard**

DeviceGuard will provide the mechanisms for

- precise policy-based control over PnP activity
- selective use of device interfaces
- control of device configuration
- analysis and control of protocol usage

DeviceGuard will cover the following device interfaces:

- Serial (RS232C)
- Parallel (IEEE 1284)
- USB
- FireWire (IEEE 1394)

The policies can regulate the usage of the device interface, taking into account such criteria as

- Protocol or protocol details (e.g.
- Device Properties (e.g. device classes and device ID)
- Properties of the user logged in (e.g. login, group)



- Computer properties (e.g. host name)
- Other properties as current date and time

## 3DGuard

Starting in second half of the second research year until the end of third research year the solution for CAD and VR data protection is developed. It will realize the automatic embedding and extraction of watermarks into and from 3D CAD data for different purposes, such as:

- Copyright Protection
- Monitoring of usage
- Access control
- Payment and Billing
- Document Management

Since these different application areas are quite distinctive a very flexible watermarking framework. Thus 3DGuard consists of a basic framework providing services as e.g. the recognition of watermarked and watermark able documents, document processing, and document management and watermarking. These basic functionalities are controlled by exchangeable security policy components, which realize a security for a specific application area. Figure 4 depicts the overall architecture of the 3DGuard solution.

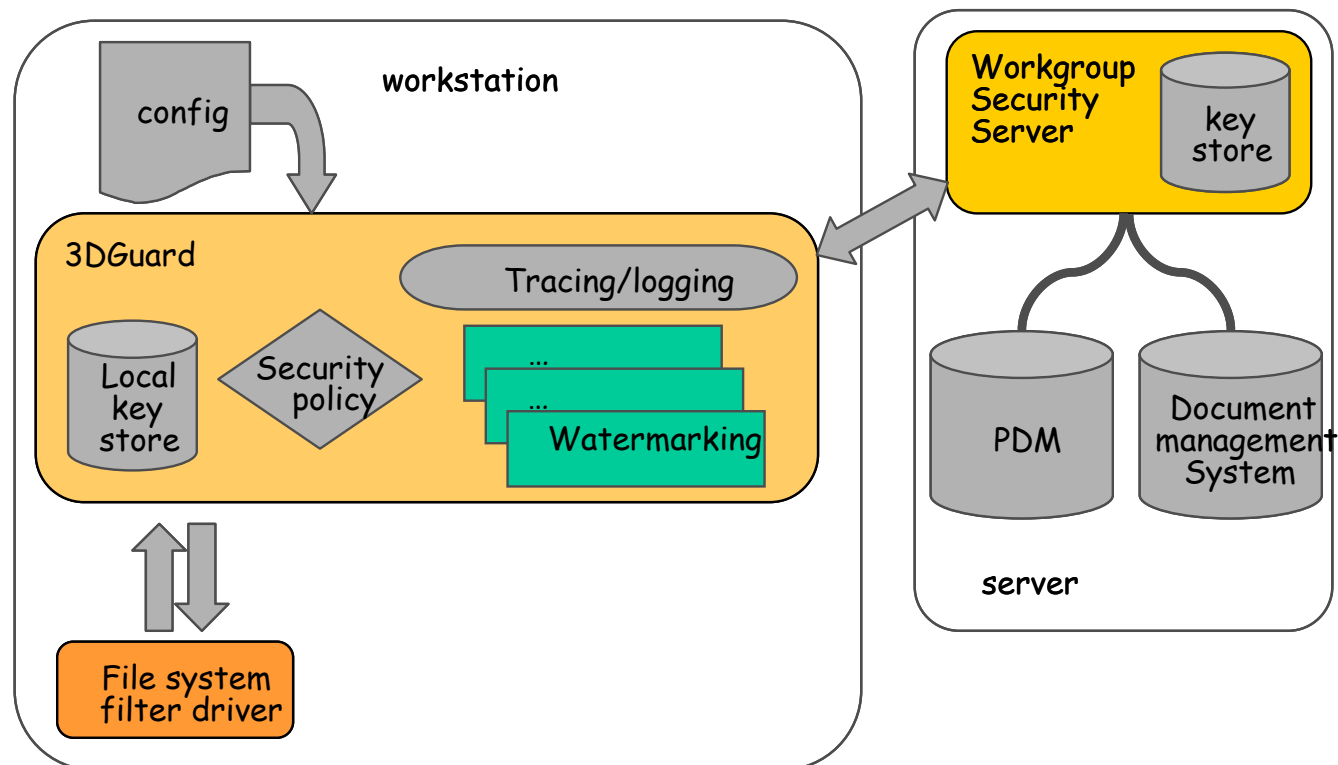


Figure 4: 3DGuard

The requirements for 3DGuard are.

- Automatic detection of watermarked and watermark able document
- Automatic pre processing of detected document, prior to the opening of the document
- Automatic post processing of detected document, after the document is closed.
- Configurable modular tool chain for pre- and post processing operations
- Support for various 3D watermarking algorithms
- Support for various security policies

In a manufacturing environment there is typically also employs some infrastructure for document and user management. 3DGuard shall make use of this infrastructure and also provide similar infrastructure for security policies. In detail:

- Provide enterprise-grade security infrastructure, as
  - ◆ Key registration and lookup
  - ◆ Policy distribution and update
  - ◆ Document tracing
- Interface to Document management system and/or PDM

The requirements concerning the watermarks are quite diverse for the different use cases. However the following issues are typical for the manufacturing environment:

- Embedding and Extraction of watermarks should be done in real time
- Embedding and Extraction of watermarks require no interaction from the user or other additional resources
- The amount of data (payload) you can embed into a watermark is quite small. Thus, the information one wants to associate with the model cannot be embedded directly. What can be embedded is only a link. Therefore 3DGuard must provide a mechanism to retrieve the additional data.
- Typically there is trade-off between the size of the payload, the strength of embedding and the quality of the data. What is the right compromise between the different parameters depends on the situation. Thus the system administrator must have a way to configure these parameters according to his needs.
- For some use cases it is essential to be able that authorized users retrieve the original (unmodified) data from the watermarked model. Thus at 3D Guard must be able to support reversible watermarks.
- There is a gap in the abstraction level. The watermarking operation are performed on file system level. The user (engineer) however thinks on level of models or even products. The watermarking policy should reflect this higher abstraction layers. This requires implementing some mapping functionality between these levels.

3DGuard will be developed in cooperation with Fraunhofer IGD, which will provide their patented 3D-watermarking technology

## **Secure Engineering Work Place**

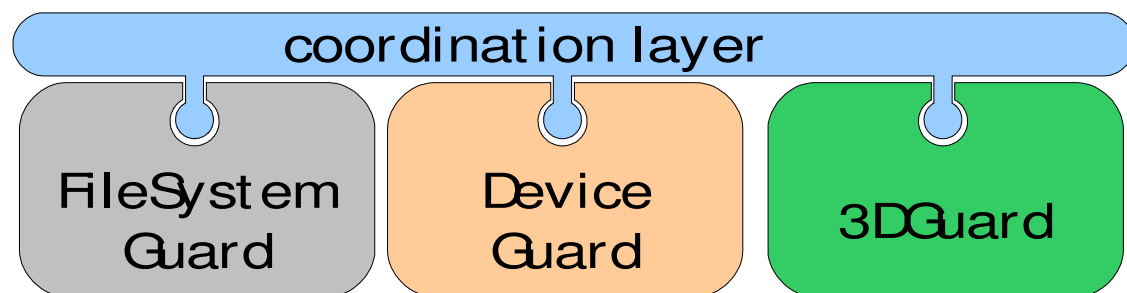
In the last research year the three solutions developed in the years before are combined into one integrated security solution, which realize a secure working place for engineer.

Simply combining the different solutions to cover the different risks will be a benefit in its own. However, the real benefit will come when on tries exploiting more synergetic effects.

A first step is the coordination of the action of different components, i.e. if one of the components detects illicit activities it can inform the other components and all of them can take collective counter measures.

Each of these solutions collects information, which is required to make policy decision. However this information collecting is restricted to the aspect they are doing the enforcement for. When combining the information from the different solutions one can get a much better insight what the user is doing and whether or not her actions are legitimate.

Instead of having a distinct security policy for each of the solutions covering a specific aspect of security, one can have now only one overall security policy. This simplifies the job of the system administration and reduces the risk of conflicts. But more important it allows the definition of more high level policy rules. So one could define a rule such as: If the user opens a file with a sensitive 3D model (3DGuard), the user is no longer allowed to exchange data with an USB stick.



**Figure 5: Secure Engineering work station**

Thus the following goals have to be met.

- Integration and harmonization of the existing components into one system
- Specification and implementation of coordination layer to
  - ♦ Allow the coordination of actions of the different solutions.
  - ♦ Improve policy decision making by combining the input from different module to obtain a more accurate model of the user activities
  - ♦ Allow the formulation of an overall security policies covering all aspect and combining different security aspects.
- Evaluation how this system meets user needs.