imc
part of Scheer

# ILS Security Whitepaper

## Information security with imc Learning Suite

im-c.com

# ILS Security Whitepaper

Information security with imc Learning Suite

Author(s): Christoph Gast
Date: 2020-07-14

| Document | Description |
|---|---|
| Version | ILS 14.5 |
| Status (Draft / Review / Finalisation) | Finalisation |
| Contact Person(s) | Chrisoph Gast |

| History | Status | Who |
|---|---|---|
| 2016-12-13 | Draft | Christoph Gast |
| 2020-07-14 | Review | Dr. Peter Zönnchen |
| | | |

**imc**
**information multimedia communication AG**
**Headquarter Saarbrücken**
**Scheer Tower, Uni-Campus Nord**
**D-66123 Saarbrücken**
**T. +49 681 9476-0 | Fax -530**
**info@im-c.com**
**im-c.com**

# Content

# 1 Information Security

This document provides an overview of imc Learning Suite and IT security. It covers individual computers, networked computers and the internet. You will find out which security problems exist and what solutions imc Learning Suite provides.

## 1.1 Confidentiality

With the electronic processing of transactions or exchange of information, it is desirable that the communication between sender and recipient remains confidential and is only accessible to the authorised persons.

### 1.1.1 Threat: Unauthorised information gain

Data confidentiality is threatened when a third party gains access to the transmitted or stored information. For instance, this can take place through intercepting communication or through direct access to a computer.

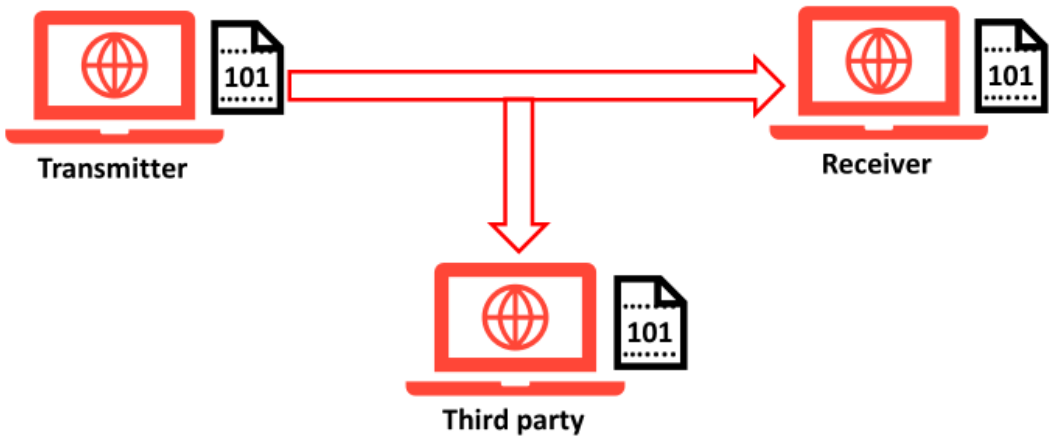


*Fig. 1.1: Unauthorised information gain*

### 1.1.2 Countermeasures: Encryption

As a countermeasure, data is often encrypted in order to make the information contained incomprehensible to third parties. imc Learning Suite facilitates secure SSL encryption between client and server and prevents interception by a third party. Further communication channels can be encrypted individually according to the security requirements. Access to computers can also be limited by means of technical measures.

## 1.2 Integrity

Integrity means that information is correct and unchanged. The recipient of a message assumes that the message reaches him just as the sender composed it.

### 1.2.1 Threat: Unauthorised modification

If a third party fraudulently modifies information this represents an attack on the integrity of the data. Modification can occur at the time of transmission or take place directly, for instance by unauthorised access to computers.


*Fig. 1.2: Unauthorised modification*

### 1.2.2 Countermeasures: Encryption and redundancy

When information is encrypted, the attacker cannot make any meaningful changes as he is not able to see the content. Another option is the used of redundancy. Through redundancy, a recipient can detect whether data has been modified. imc Learning Suite secures all communication through the use of SSL encryption and also uses the token procedure and a secure session procedure. By using this procedure, communication between client and server is additionally protected; manipulation of data can be detected in this way and can be prevented by the use of appropriate countermeasures.

## 1.3 Authenticity

Authenticity is the assurance that information originated from a certain person.

### 1.3.1 Threat: Unauthorised creation

When data is generated in such a way that this data is assigned to the incorrect person, this represents an attack on the authenticity. For instance, transfers can be executed at the expense of an uninvolved person because a third party has impersonated this person.


*Fig. 1.3: Unauthorised creation*

### 1.3.2 Countermeasures: Securing identity

There are a lot of measures that should secure the identity of a person. Some of them are easier to crack, for instance, the authentication with username and password, others are more secure, like e.g. a digital signature or a fingerprint. Besides encryption and secure login data, imc Learning Suite focuses on the token procedure which prevents manipulation of identity data and makes it visible in case of emergency.

## 1.4 Availability

Availability means the provision and functionality of data, computers and communication means.

### 1.4.1 Threat: Unauthorised interruption

If an IT system is not accessible is only partly runs or information is not accessible, this can have serious economic consequences. A denial-of-service attack for instance, represents un-authorised interruption. Here, systems are intentionally overloaded and are no longer available or only available for a limited period.


*Fig. 1.4: Unauthorised interruption*

### 1.4.2 Countermeasures: Avoidance of "single point of failure"

Systems which cannot be paralysed by an error at one single point (single point of failure) are better protected against unauthorised interruption. This can be achieved through the use of high availability, redundant systems. When a system fails, a second, identical system steps into the breach. imc Learning Suite supports different system architectures which avoid a single point of failure. Thus, high system availability can, for instance, be achieved through clustering. Clustering means that individual system components are transferred onto separate, networked servers. Suggestions for possible system architectures are described in the technical whitepaper for imc Learning Suite.

## 1.5 Information on security and vulnerabilities

Further information on frequent vulnerabilities in software products can be found under the following links:

- Federal Office for Information Security: Comprehensive information on vulnerabilities and measures that one can take to protect themselves against security risks. http://www.bsi.de
- National Vulnerability Database: Database listing concrete vulnerabilities in software products. http://nvd.nist.gov/
- The Open Source Vulnerability Database: Database listing vulnerabilities in open-source software products. http://osvdb.org/

# 2 Standards

## 2.1 SSL/TLS

Transport Layer Security (TLS) is better known as Secure Sockets Layer (SSL). Since version 3, SSL has developed further as TLS. TLS is an encryption protocol which facilitates secure data transmission between two hosts.

The benefit of SSL protocol is that any protocol can be implemented based on SSL protocol. An example of this is the HyperText Transfer Protocol Secure (HTTPS) which is identical to HTTP; the only difference being that the transmitted data is encrypted using TLS. HTTPS protocol is used on the internet for authentication and for encryption of communication between browser and web server.

imc Learning Suite provides the opportunity to encrypt the communication between client and server using SSL. This allows different encryption algorithms to be implemented and the certification key can be selected according to the security requirement. Furthermore, imc Learning Suite supports so-called Extended Validation SSL Certificates (EV-SSL). For an EV-SSL certification, the client must undergo further inspection by a certification body. Identity and business address of the client are checked amongst other things. Websites with EV-SSL-certification are identified in the browser by green highlighted company name in the address bar. EV certificates are used in online banking, for example.

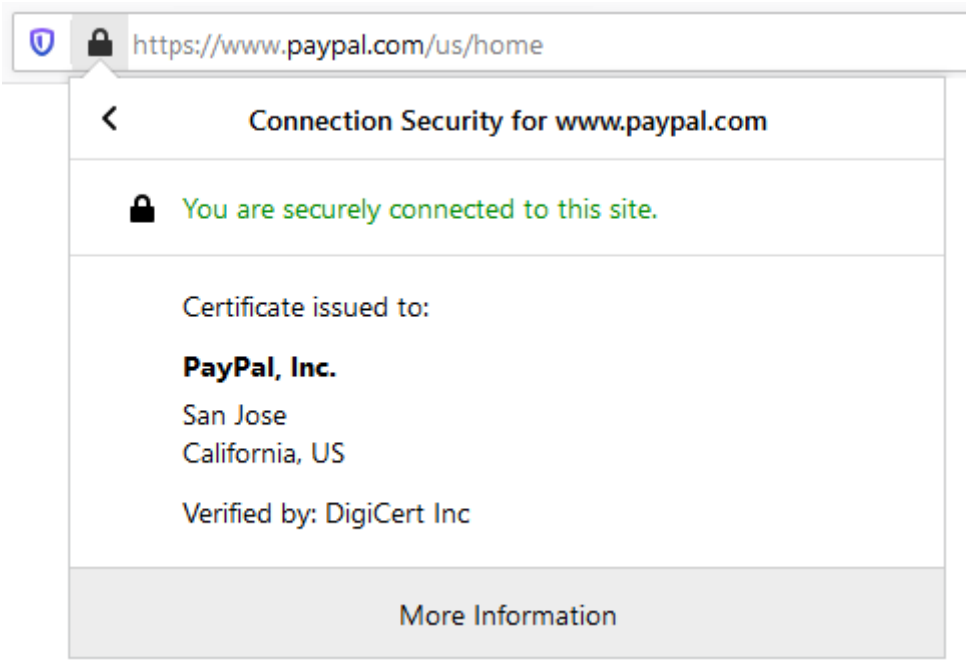


*Fig. 2.1:Example of a website with EV-SSL certification*

### In general facilitates SSL

- authentication of the communications partner,
- confidentiality of data through encryption,
- integrity of data by verifying hash values (hash value = checksum).

## 2.2 MD5/SHA2

Message-Digest Algorithm 5 (MD5) is a popular, rapid cryptographical hash function. Hash functions map a character sequence of any length onto a character sequence of a fixed length. MD 5 generates a hash value of 128 bit. The 128 bit hash values are normally issued as 32 digit hexadecimal numbers (e.g. 4eff7d0e702050df5fc72e2b8946ab41).
SHA-2 (Secure Hash Algorithm 2) is a set of cryptographic hash functions designed by the NSA. SHA stands for Secure Hash Algorithm. Cryptographic hash functions are mathematical operations run on digital data; by comparing the computed "hash" (the output from execution of the algorithm) to a known and expected hash value, a person can determine the data's integrity. A key aspect of cryptographic hash functions is their collision resistance: nobody should be able to find two different input values that result in the same hash output.
imc Learning Suite uses the MD5 or SHA2 (256bit) procedure for functions which need one-way encryption. With one-way encryption, a text is simply encrypted but no longer decrypted. In this way, it can be determined whether a user is in possession of a certain text to be encrypted (e.g. password). With password verification in imc Learning Suite, the encrypted hash values of the entered and saved password are compared to each other. The procedure is strengthened even more through multiple use of security measures.
The hash algorithm can be configured in imc Learning Suite in the configuration file clix.conf (section "security","passwordHashAlgorithm"). Possible values are MD5 and SHA-256.

## 2.3 DES

The Data Encryption Standard (DES) is a widely used encryption standard. The key length is 56 bit, however it can be extended through multiple application. DES is used for voice encryption for instance. In Germany, the German federal and state constitution protection agencies use the DES standard.
imc Learning Suite uses DES for secure data exchange. Data is encrypted by imc Learning Suite with the help of the DES standard before it is transmitted.

## 2.4 OWASP

The Open Web Application Security Project (OWASP) is a non-commercial organisation. The aim of OWASP is to improve software security. OWASP draws attention to frequent vulnerabilities and enables these to be combated. Further, OWASP defines standards for secure development and

application of software. An important OWASP publication is the Top 10 most serious security breaches of web applications.
imc factors in the OWASP standards when further developing imc Learning Suite. The tools and libraries recommended by OWASP are used in order to adapt the security of imc Learning Suite to the required standards; imc subjects imc Learning Suite to permanently new tests and thus ensures that the level of security are adhered to overall patch and release cycles and is increased through additional security measures.

# 3 imc Learning Suite security measures

imc continues to develop imc Learning Suite so that the highest standards can be achieved in terms of IT security. Below, you will find a selection of security measures integrated into imc Learning Suite.
Advanced concepts for security experts can be introduced in the context of a non-disclosure agreement.

## 3.1 Authorisation and visibility concepts

The following chapter describes measures which users of imc Learning Suite can implement themselves or which have to do with user input into the system.

### 3.1.1 Profile data

At different places in imc Learning Suite, user profiles can be displayed or users can input data. Profiles contain personal information on individual people like for instance their name or email address. For instance, a user can record the contact details of other users or search for people in their address book.
imc Learning Suite offers the opportunity to display different data according to context and user or to make different input fields available. Thus, you can determine precisely which personal data is to be entered in imc Learning Suite and which of these profiles is visible to other users. Thus, imc Learning Suite supports different levels of confidentiality which is flexibly adaptable depending on the context.

### 3.1.2 Organisational chart

Each organisation or company who uses imc Learning Suite has its own internal structure. This structure can be illustrated in detail via client, group and approval management.

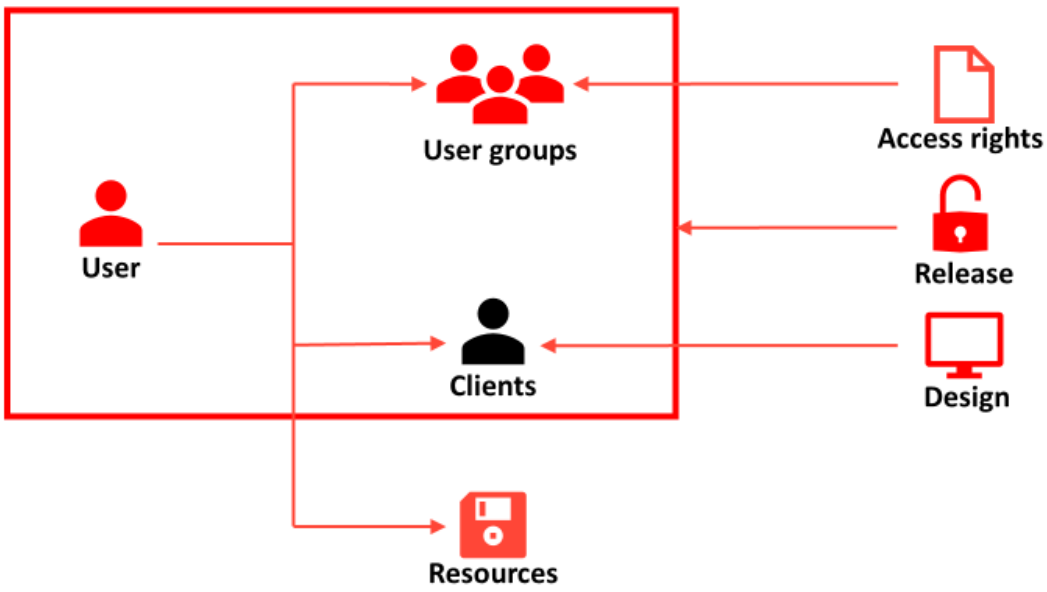


*Fig. 3.1: Organisational chart*

### Clients

Clients serve to divide a single physical system into multiple partial systems. The sub-systems can for instance, represent different departments within an organisation and can also differ in design. Different settings in imc Learning Suite can be made client-specific such as, for instance, the determination of a recipient group for a message. Any number of clients can be created.

### User groups

Individual users can be broken down into user groups. Via user groups, it is controlled which functions are accessible to members of a user group. For example, it is possible to determine which navigation menus are visible and which functions the group members can find there. Any number of user groups and sub-groups can be defined.

### Releases (ACL)

Via an Access Control List (ACL), the releases of objects for users, user groups and clients are determined. Release represents an access right. For each object in imc Learning Suite (e.g. a certain type of content) it can be defined which users, user groups or clients have access to this object. For each object, only those specific rights which are required for administration clearances exist, for example, "Edit", "Delete" or "Release".

**Organisational chart**

Through the combination of client and group affiliation and release, it can be defined for each person which content this person can see, how the content is presented and to which functions the person has access. The imc Learning Suite organisational chart thus supports optimal confidentiality and content integrity. Users only see the content which is destined for them and can only make changes or access functions to which they have access.

### 3.1.3 Passwords

**Autocomplete**

Login to imc Learning Suite takes place using a unique combination of user name and password. Depending on how the used browser is set up, this login data is possibly saved on the browser. In this way, the user does not need to enter the login data every time, rather the browser fills in the login fields automatically (autocomplete = auto-completion). The disadvantage of this is that attackers can possibly upload and misuse this saved login data.
imc Learning Suite prevents automatic saving of login data in the browser. Thus, it makes no difference whether users have activated the autocomplete function in the browser or not. The passwords of the internet sites remain unaffected.

**Identical passwords**

If a user creates a password for their imc Learning Suite access, the password is saved in encrypted format in the imc Learning Suite database (as a so-called hash value). If different users randomly select identical passwords, then normally the encrypted versions of these passwords are also identical. Thus, for example, an administrator who has access to the imc Learning Suite database can compare encrypted passwords and draw conclusions from them.
In order to counteract this, imc Learning Suite adds a personal "Salt" to each password. As Salt, one signifies a random sequence of characters in the computer cryptography. This sequence of characters is linked to the password which means that the encrypted stored passwords are never identical, even if the passwords appear to be identical in plain terms.

### 3.1.4 Denial of Service (DoS)

Logging into imc Learning Suite is executed by using a username and password. If a user falsely inputs his passwords several times in succession, imc Learning Suite automatically locks the user account for security reasons (Denial of Service). This locking of the login has consequences for individual users of temporary restricted availability. However, it is important that the system with the ability to lock logins is protected again Brute-Force attacks against the passwords. Brute Force means that an attacking server tries passwords until he has eventually cracked one of the passwords and thus can potentially cause a great deal of damage. Locking the login prevents this.
The number of login attempts until locking occurs and the period up to automatic unlocking can be freely configured.

### 3.1.5 Audit Log

In the audit log, participant-related data such as, for example, the booking date or the booking status of a course is managed and logged. Changes which were brought about by the course participant are likewise logged in the audit log.

The audit log is usually only accessible to trained administrators. With the audit log, an administrator can trace when and where and by which person changes were made. If these changes were unintentional, for example, if a participant has accidentally ended a course early, these changes can be reversed.

With the audit log, imc Learning Suite administrators have access to an important tool through which data integrity can be ensured.

# 4 Penetration tests

A penetration test, also referred to as a Pen Test, is a comprehensive security test of an IT system or software. Based on the methods which a possible attacked would use in order to penetrate a system, potential vulnerabilities are systematically revealed.
The purposes of a penetration test are

- to detect weak spots,
- to detect errors which can occur through incorrect operation,
- to increase security.
- to confirm IT security through a third party.

imc regularly has penetration tests performed for imc Learning Suite. The results of the tests are incorporated into new patches, service packs and releases of imc Learning Suite.