Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI

Bundesamt für Gesundheit BAG
Direktionsbereich Gesundheitspolitik

SR 816.11.n / Anhang 8 der Verordnung des EDI vom ... über das elektronische Patientendossier

Vorgaben für den Schutz der Identifikationsmittel

Protection Profile for Electronic Means and their Authentication Procedures

---

Version: 1.0 22.03.2016

Inkrafttreten: …

Table of Contents

PP Introduction

The Swiss Federal Law on Electronic Health Records (FLEHR) requires a strong authentication of identity for patients and healthcare professionals in order to access the Swiss Electronic Health Record (EHR). The Federal Council sets the requirements in relation to electronic identities and the issuing process for Electronic Identification Means (EIM) in detail. In this regard, EIM are used to identify patients and healthcare professionals to access the Swiss national electronic health record (EHR) via an access portal that is operated by communities (association of health professionals) and reference communities (communities with additional responsibilities related to the establishment of an account for the Electronic Patient Record). To assure a high confidence in the claimed identity of patients and healthcare professionals, the related processes for instantiation and issuance of identification means such as identity proofing and verification or credential issuance have to comply with the requirements for the level of assurance 3 as defined in ISO/IEC 29115:2013

The Protection Profile for Electronic Identification Means and their Authentication Procedures is based on the Regulations on the Electronic Patient Record (EPDV). It defines a set of requirements that are expected to be fulfilled by all products that can perform electronic identification and authentication to access the Swiss national EHR. The evaluation of EIM according this protection profile is part of the certification process of communities and reference communities, respectively.

1.1 PP Reference

Title:	Protection Profile for Electronic Identification Means and their Authentication Procedures
Version:	1.0
Date:	23.03.2016
Issuer:	Swiss Federal Office of Public Health
Evaluation Assurance Level	The assurance level for this PP is EAL2
CC Version	V3.1 Revision 4

1.2 TOE Overview

This protection profile defines the security objectives and requirements for EIM including their authentication procedures required to access the Swiss national EHR.

1.2.1 TOE definition

The Target of Evaluation (TOE) addressed by this protection profile comprises the components that are relevant to instantiate as an EIM towards relying parties (RP) in the EPDV context, namely it provides the following:

- An Identity Provider (IdP) for identification and authentication of registered users.
- Web services / middleware / internet visible access portal for authentication provided by IdP.
- Web service / middleware to create secure channel between IdP and service provider (i.e. community portal for patients and healthcare professionals) provided by IdP.
- Web service / middleware provided by service provider (i.e. community portal for patients and healthcare professionals) to receive authorization response from secure channel from IdP.
- Devices of multiple variety (e.g. smartcard, mobile devices) carrying tokens (e.g. application on mobile device) and/or credentials (e.g. public and secret key material, authentication credentials).
- Secure handover of randomized and time limited session from service provider to device (e. g. secure browser redirect or equivalent level)

1.2.2 TOE Usage

Electronic identification means comprises one or more token that are secured by a device. Each token may hold a credential, that is used by the IdP to authenticate the user's identity based on possession and control of the corresponding token. Figure 1 shows the steps required to authenticate patients and healthcare processionals to an access portal of communities.

In the first step, the holder of the token authenticates himself to the IdP (1) which provides a defined interface for that purpose. Specifically, this means an IdP-initiated approach where the IdP refers to service provider or relying party and, thus, the claimant may choose a specific context (2). In the next step, the IdP verifies the credentials of that user and after successful verification, the IdP transmits a proof of identity to the access providing system of the (reference-) community (3). The connection between IdP and service provider (SP) has to be established via secure channel. This channel shall also be used for initial notification of an approved patient's identity to the reference community of the patient. Although the IdP authorizes patients and healthcare professionals in order to grant access to the EHR, fine-grained permission control is left to the reference community.

To access the EHR, the session has to be handed over from the service provider to the IdP or the user's device (3,4). Afterwards, the user has access via the interface to the services authorized for this user in the (reference-) community.

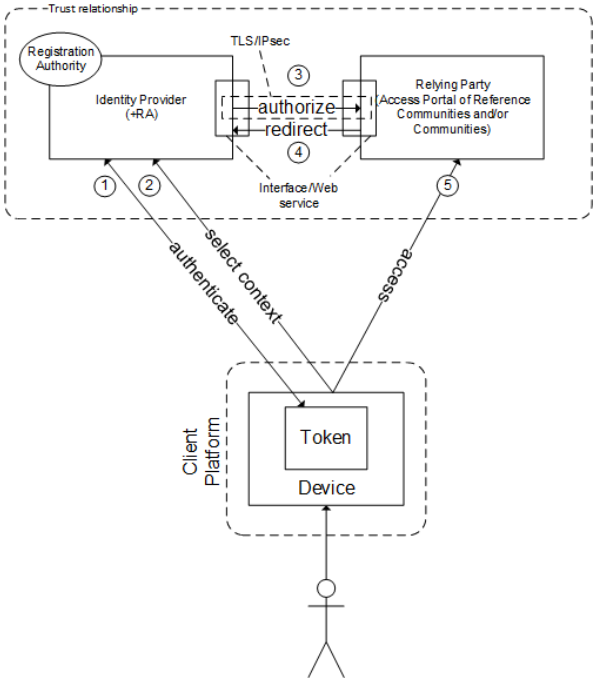

Figure 1 Usage of the TOE

1.3 Operational Environment

EIM have to be compliant with a specific level of assurance (LoA 3) as defined by ISO/IEC 29115:2013 [9]. It is assumed that EIM meet all necessary requirements related to enrolment, credential management and entity authentication such that there is a high confidence in the claimed or asserted identity of patients and healthcare professionals being allowed to access the EHR.

1.4 Physical Protection of the TOE

The physical protection is mainly provided by the TOE environment. This specifically covers the following scenarios:

- Access to the TOE infrastructure is not sufficiently restricted and the attacker gains unauthorized access to the server environment.
- The device is stolen and manipulated an attacker.

1.5 Assets

The assets to be protected by the TOE are data listed in Table 1. Assets of the TOE are divided into TSF and User data and the security services provided by the TOE as defined above. The data assets known to the TOE environment like public keys shall be protected by the TOE environment as well.

TSF data / User Data	Data	Description
User data	Device / Token with secret/public credential	A device that carries a secret/public credential of an individual user • Disseminated beforehand in a rollout process • Activation data or password is only known to the user Note that the device could be of multiple variety (e. g. Chipcard, Handheld-Device, Harddisk).
User data	Activation data for token	An activation secret for the token.
User data	Credential for web portal	A credential that is used for additional login into the access portal of the reference community.
User data	Secret and private credential of the user (on token)	The token stores secret and private credential of a user to authenticate the user has to be stored in a confidential and integrity protected way by the TOE.
User data	Reference of user credential	The IdP stores reference of the credential of a user to authenticate the user has to be stored in a confidential and integrity protected way by the TOE.
User data	Token output / authenticator	Authentication data that is transferred from the Token to the IdP Raw or transformed, e.g. in form of a cryptographic expression
User data	Identification Data	A unique tuple that identifies a user e.g. GLN, given birthname, birthdate, etc.
TSF data	Cryptographic Key Material for Channels	All cryptographic key material that is used to establish secure channels for communication between parts of the TOE or between the TOE and other trusted components as well as the browser.
TSF data	Claimant ID	A unique ID provided by the IdP to identify the claimant unanimously.
TSF data	Assertion Data	Any SAML assertion defined and generated by the TOE.

Table 1 Assets of the TOE divided into TSF and User data.

1.6 External Entities and Subjects

This protection profile considers the following subjects and external entities:

Entity	Description
User	A patient, a patient's representative, a Healthcare professional or an authorized supportive persons with access to the EDP, i.e. that have a identification token beforehand.
Trusted Users	Administrators, Operators and Security Information Officers that have privileged access rights to the EIM platform.
Temporary privileged users	Users that might have temporary privileged access rights, e.g. developers, support persons and auditors.
Test users and functional users	Technical users that might exist for management of the platform.
Attacker	A human, or a process acting on his behalf, located outside the TOE. The main goal of the attacker is to access or modify security relevant data.
Service Provider (Relying Party)	Data storage and infrastructure on (reference-) community site that is connected to the EIM and provides the access control for identified users (authorization control in accordance with the regulation). Additionally a secure channel exists between the (reference-) community infrastructure and the EIM.
RA (Registration Authority)	A trusted entity that establishes and vouches for the identity of a Subscriber/Claimant to an IdP. The RA may be an integral part of an IdP, or it may be independent of an IdP, but it has a relationship to the IdP(s).
IdP (Identity Service Provider)	A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The IdP may encompass Registration Authorities and verifiers that it operates. An IdP may be an independent third party, or may issue credentials for its own use.
Subscriber/Claimant	A user after successful identification and registration.
Client_Platform	The platform environment from which the user requests an identification process at the IdP. (e.g. for a user's PC with browser for redirect to the community access portal and a connected mobile device with the token).
Service desk	Portal within the IdP for user help and revocation requests

Table 2 External Entities and Subjects

2 Conformance Claims

- This PP has been developed using Version 3.1 R4 [1], [2], [3] of Common Criteria [CC].
- This PP does not claim conformance to any other PP.
- This PP requires strict conformance of any PP/ST to this PP.

This PP claims an assurance package EAL2 as defined in [CC] Part 3 for product certification.

3 Security Problem Definition

The Security Problem Definition is the part of a PP, which describes

- Assumptions on security relevant properties and behavior of the TOE's environment;
- Organizational security policies, which describe overall security requirements defined by the organization in charge of the overall system including the TOE. In particular this may include legal regulations, standards and technical specifications;
- Threats against the assets, which shall be averted by the TOE together with its environment.

3.1 Assumptions

Assumption	**Description**
A.Personal	It is assumed that background verification checks on all candidates for employment, contractors, and third party developers are carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. It is assumed that all employees and contractors understand their information security responsibilities, are authorized and trained for the roles for which they are considered and are aware of information security threats. Healthcare professionals and patients are assumed to always act with care and read the existing guidance documentation of the corresponding part of TOE. It is assumed, that holders of devices/tokens and other computing platforms keep secret activation/authentication data confidential, ensuring that it is not divulged to any other parties and avoid keeping a record on paper, in a software file or on a hand-held device, unless this can be stored securely and the method of storing has been approved.
A.AccessManagement	An Access Management is in place to control the allocation of access rights for authorized user access and to prevent unauthorized access to information systems and physical premises.
A.Physical	It is assumed, that the components of the TOE except for the enrolled device/token are operated in a secure area and protected against physical manipulations.
A.Monitoring	It is assumed, that information processing systems on the service providing part of the TOE are monitored and user activities, physical access to secure areas, exceptions, and information security events are recorded to ensure that information system problems are identified.

	It is assumed that the clocks of all relevant information processing systems are synchronized with an agreed accurate time source.
A.Malware	It is assumed, that that information processing systems on the service providing part of the TOE and its computing environment is protected against malware based on a malware detection and repair system service and information security awareness is introduced and practiced. It is also assumed, that a vulnerability management to prevent exploitation of technical vulnerabilities is established and maintained.
A.ClientPlatform	It is assumed, that the computing environment on which a part of the TOE is installed or interacts and has access to the services provided by the TOE, is protected against malware, its components have a current patch status and is not used in the administrator mode. It is assumed, that this computing environment is a general home-type environment. This means low physical security measures.
A.Identification	It is assumed that the claimant is carefully identified and well informed concerning practicing security awareness.
A.CredentialHandling	It is assumed that a mechanism to ensure that a credential is provided to the correct entity or an authorized representative is implemented. It is assumed that procedures ensure that a credential or means to generate a credential are only activated, if it is under the control of the intended entity. Therefore the device/token is protected against unauthorized access with activation data only known to the claimant. In the case of revocation due to compromise or loss of device/token, it is assumed, that the claimant informs immediately the service desk of the IdP through appropriate channels.
A.TrustedCommunityEndpoint	It is assumed, that the community provides a trusted endpoint for defined secure communication with the IdP.

Table 3 Assumptions

3.2 Organizational Security Policies (P)

The TOE and/or its environment shall comply with the following Organizational Security Policies (P) as security rules, procedures, practices, or guidelines imposed by an organization upon its operation.

Policy	Description
P.Audit	The security relevant events (internal to the TOE or due to the communication flows) shall be recorded and maintained and reviewed. The audit trail analysis is executed in order to hold the authorized users accountable for their actions and to trace attack attempts from networks. At minimum, the following items should be logged: - user IDs - dates, times, and details of key events - terminal identity - records of successful and rejected system access attempts - changes to system configuration - use of privileges network addresses and protocols
P.Crypto	State of the art recommended cryptographic functions shall be used to perform all cryptographic operations (e.g. NIST or other applicable guidance and recommendations). At least the following or stronger cryptographic algorithms shall be used: - SHA-2 - AES: n ≥ 256 - RSA: n ≥2048 - ECDSA: n ≥ 224
P.AccessRights	A defined management of admission to TOE and network resources shall be established that grants authenticated users access to specific resources based on policies and permission levels, assigned to users or user groups. The access control shall include an authentication, which proves the identity of the user or client entity attempting to log in. Administrative privileges allow users the right to make any and all changes on the TOE, including setting up accounts for other users and change SFR specific settings. The allocation and use of system administration privileges shall be more restricted and controlled.
P.Hardening	A defined policy for hardening the TOE shall be established and processes shall be implemented for securing the systems within the TOE by reducing its vulnerability. To achieve this, an effective vulnerability and patch management shall be established, unnecessary software shall be removed, unnecessary services shall disabled or removed and access rights and access to resources shall be strongly restricted and controlled.
P.Assertion	SAML-Token has to comply with the specification given in section 6.3. The IdP information processing system shall contain a component to generate unique reference identifiers. A time restricted SAML-Token issued by the IdP shall be digitally signed with an enhanced signature by a certified certificate service provider.
P.TrustedCommunityEndpoint	A trusted community endpoint for the secure communication between the IdP and the Community shall be established as defined in section 6.3.

Table 4 Description of the organizational security policies the TOE and its environment shall comply with

3.3 Threats

This section describes the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats result from the assets protected by the TOE and the method of OE's use in the operational environment. The threats described in chapter 10.3 of the ISO/IEC 29115 are fully covered and extended by the following threats.

Threat	**Assets/ Security Goals / Adverse Action / Attacker**
T.CompromiseToken/Credential Compromise of a device/token and their credentials	Asset: Secret and private credential of the claimants device/token Security goal: The TOE and therefore all assets of the TOE Adverse action: Exposition of credential stored on a device/token - An attacker causes a IdP to create a credential based on a fictitious subscriber/claimant - An attacker alters information as it passes from the enrolment process to the credential creation process. - An attacker obtains a credential that does not belong to him and by masquerading as the rightful claimant causes the IdP to activate the credential. - An attacker has access to secret credentials stored on a device/token of a registered claimant with a weak credential protection mechanism and is therefore able to export or copy these secret credentials. Subsequently he is able to use these secret credentials for masquerading the rightful claimant (direct use or duplication of the token). - An attacker has either direct access to the activation data by breaking a weak protection mechanism or he can apply analytical methods outside the authentication mechanism (offline guessing) supported by a weak protection mechanism of the device/token. - An attacker can capture activation data or credentials by sending disguised malware as applications (e.g. keystroke logging software), which can be stored on a device. - The dissemination of revocation information is not timely leading to a threat of device/token with revoked credentials still being able to authenticate before the IdP updates the latest revocation information. Attacker: An Attacker alters information during the enrolment process of a device/token or gains access to a credential of a registered claimant and impersonates him or her either by credential tampering, credential disclosure, credential duplication, delayed credential revocation or offline guessing.
T.Token/CredentialTheft	Asset: Secret and private credential of the claimants device/token Security goal: The TOE and therefore all assets of the TOE

	Adverse action: A device/token that generates or contains credentials is stolen by an attacker Attacker: If an attacker also knows the activation data or has direct access to the activation data by breaking a weak protection mechanism or can apply analytical methods outside the authentication mechanism (offline guessing) favored by a weak protection mechanism of the device/token, he gain an authenticated access to the TOE and therefore all assets of the TOE.
T.WebPlatformAttacks	Asset: The TOE and therefore all assets of the TOE. Security goal: Confidentiality and integrity of the assets. Adverse action:. - Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities. - Cross-Site-Scripting (XSS) flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the claimant's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites. - A Cross-Site Request Forgery attack (CSRF) forces a logged-on claimant's browser to send a forged HTTP request, including the claimant's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the claimant's browser to generate requests the vulnerable application thinks are legitimate requests from the claimant. - Injection flaws, such as SQL, OS-Command-Shell, XPATH and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization. - Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect claimants to phishing or malware sites, or use forwards to access unauthorized pages. - Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

	Attacker: - Not correctly implemented authentication and session managements allow an attacker either capture or bypass the authentication methods that are used by a web application. He is able to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users identities (Unencrypted connections, predictable login credentials, vulnerable and unprotected session handling, no or too long timeouts, etc.) - An attacker can inject untrusted snippets of JavaScript into an application without validation. This JavaScript is then executed by the claimant who is visiting the target site. There are 3 primary types: In Reflected XSS, an attacker sends the claimant a link to the target application through email, social media, etc. This link has a script embedded within it which executes when visiting the target site. In Stored XSS, the attacker is able to plant a persistent script in the target website which will execute when anyone visits it. With DOM Based XSS, no HTTP request is required, the script is injected as a result of modifying the DOM of the target site in the client side code in the claimant's browser and is then executed. - Cross-Site Request Forgery (CSRF) is a web application vulnerability that makes it possible for an attacker to force a claimant to unknowingly perform actions while they are logged into an application. Attackers commonly use CSRF attacks to target sites such as cloud storage, social media, banking and on-line shopping, because of the user information and actions available in these applications. - All injection attacks involve allowing untrusted or manipulated requests, commands, or queries to be executed by a web application. An attacker wants to perform SQL inject they could write a SQL query to replace or concatenate an existing query used by the application, using specific characters like to bypass the existing query-logic. For an OS commanding injection an attacker can include a shell command within their injection using specific characters to include attacker's commands. Each attack could be tailored to the attacker's goal, the target server's infrastructure, and which inputs can bypass the application's existing logic. XPATH is the query language used to parse and extract specific data out of XML documents, and by injecting malicious input into an XPATH query, an attacker can alter the logic of the query. This attack is known as XPATH injection. - Applications that redirect after a successful authentication to another location by sending a redirect header to the client in an HTTP/HTTPS response, an attacker can without proper validation redirect claimants to phishing or malware sites, or use forwards to access unauthorized pages. - The web application needs to verify the request at the UI level, as well as the backend function level. An attacker will ignore the UI and a forge requests that access unauthorized functionality.

T.SpoofingAndMasquerading	Asset: The TOE and therefore all assets of the TOE. Security goal: The confidentiality and integrity of the assets. Adverse action: Spoofing and masquerading refer to situations in which an attacker impersonates another entity in order to launch attacks against network hosts, steal data, spread malware or bypass access controls. This may be done by making use of the credential(s) of an entity or otherwise posing as an entity (e.g. by forging a credential). Attacker: An attacker impersonates an entity spoofs one or more biometric characteristics that matches the pattern of the entity (by creating a “gummy” finger, recording voice, etc.) IP spoofing attacks can be used to overload targets with traffic or bypassing IP address-based authentication, when trust relationships between machines on a network and internal systems are in place. Such spoofing attacks impersonate machines with access permissions and bypass trust-based network security measures. An attacker spoofs a MAC address by having its device broadcast a MAC address that belongs to another device that has permissions on a particular network. In a DNS server spoofing attack, an attacker is able to modify the DNS server in order to reroute a specific domain name to a different IP address. This attack can also be used to masquerade a legitimate IdP with an attackers IdP or masquerade a legitimate software publisher responsible for downloading on-line software applications and/or updates by a faked downloading service.
T.SessionHijacking	Asset: Credentials, Session-IDs and other user data Security goal: The confidentiality and integrity of the assets Adverse action: An Attacker is able to intercept successful authentication exchange transactions between the claimant and the IdP and to steal or predict valid session data to gain compromised/unauthorized access to the web portal of the service provider. Without effective countermeasures, such attacks could be successfully performed using methods like Session Sniffing, Client-side attacks (XSS, malicious JavaScript Codes, Trojans, etc), Man-in-the-middle attacks, Man-in-the-browser attacks. Attacker: An Attacker is able to take over an already authenticated session by eavesdropping on or predicting the value of authentication data used to mark HTTP/HTTPS requests sent by the claimant to the IdP and subsequently gain compromised/unauthorized access to the web portal of the service provider. An attacker logs into a vulnerable application, establishing a valid

	session ID that will be used to trap the claimant. He then convinces the claimant to log into the same application, using the same session ID, giving the attacker access to the claimants account through this active session.
T.OnlineGuessing	Asset: User credentials Security goal: The confidentiality of assets Adverse action: An Attacker performs repeated logon trials by guessing possible values of the token authenticator. Attacker: An Attacker navigates to a web page and attempts to log in using brute force methods based on specific dictionaries.
T.ReplayAttack	Asset: Credentials, authentication exchange data Security goal: The confidentiality of assets Adverse action: An Attacker is able to replay previously captured messages (between a legitimate Claimant and an IdP) to authenticate as that Claimant to the IdP. Attacker: An Attacker captures a Claimant's credential or session IDs from an actual authentication session, and replays it to the IdP to gain access at a later time.
T.Eavesdropping	Asset: Credentials, authentication exchange data and other user data Security goal: The confidentiality of communication channels and assets of the TOE Adverse action: An Attacker listens passively to the authentication transaction to capture information which can be used in a subsequent active attack to masquerade as the Claimant. A way to achieve this, the attacker positions himself in between the Claimant and the IdP, so that he can intercept the content of the authentication protocol messages. The Attacker typically impersonates the IdP to the Claimant and simultaneously impersonates the Claimant to the IdP. Conducting an active exchange with both parties simultaneously may allow the Attacker to use authentication messages sent by one legitimate party to successfully authenticate to the other. Attacker: An Attacker captures the transmission credentials or Session IDs

	from a Claimant to a IdP.
T.Configuration	Asset: The TOE and therefore all assets of the TOE. Security Goal: Confidentiality and integrity of the assets. Adverse action: An unauthenticated or authenticated attacker might exploit a weakness resulting from a wrong configuration setting, incomplete deployment or not up-to-dated software (libraries, frameworks, and other software modules, almost always running with full privileges) of TSF components of the TOE (applications, frameworks, application servers, web servers, database servers and platforms) Attacker: An unauthenticated or authenticated attacker is able to exploit a weakness by wrong configuration setting, incomplete deployment or not up-to-dated software to expose confidential information about user data or TSF data.
T.DoS	Asset: The TOE and therefore all assets of the TOE. (The availability of the TOE). Security goal: The Denial of Service (DoS) attack is focused on making TSF components of the TOE (site, application, server) unavailable for the purpose there were designed. Adverse action: An attacker is able to manipulate network packets, programming, logical, or resources handling vulnerabilities, etc. Attacker: An (unauthenticated) attacker is able to start a DoS attack on the external interfaces of the TOE (namely browser interface and web service) so that a service receives a very large number of requests and may cease to be available to legitimate users. An (unauthenticated) attacker is also able to stop a service, if a programming vulnerability is exploited or to slow down using too much service handles.

Table 5 Threats

4 Security Objectives

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment.

4.1 Security Objectives for the TOE

This section describes the security objectives for the TOE and addresses the aspects of identified threats to be countered by the TOE and organizational security policies to be met by the TOE. The security objectives describe the protection of the primary assets as User Data and the secondary assets as TOE security functions data (TSF data) against threats identified in TOE environment.

O.Integrity	The TOE shall protect against either intentional or accidental violation of user and TSF data integrity (the property that data has not been altered in an unauthorized manner) or violation of system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).
O.Confidentiality	The TOE shall protect user and TSF data against intentional or accidental attempts to perform unauthorized access. The TOE shall protect confidentiality of user and TSF data in storage, during processing and while in transit.
O.Availability	The TOE shall ensure the availability of services provided by the TOE and the TSF to authorized users (e.g. the IdP is unavailable to subscribers as a consequence of a DoS attack or insufficient scalability).
O.Accountability	The TOE shall trace all actions of an entity uniquely to that entity. The TOE shall record user activities, exceptions, and information security events and shall keep these for an agreed period to assist in future investigations and in access control monitoring.
O.Authentication	Towards the service provider: All messages between IdP and their relaying parties shall be digitally signed to guarantee the authenticity and validity shall be time limited. Towards the client platform: The TOE shall provide either a token with two or more authentication factors (multifactor token) or a combination of a single-factor token and at least another token transmitted on a separate channel for authentication. The factors shall comply with the requirements of ISO 29115.
O.Secure_Communication	The TOE shall support secure communication for protection of the confidentiality and the integrity of the user data and TSF data received or transmitted. Further nonces, challenges or timeliness shall be used for freshness of each transaction.
O.Cryptographic_Functions	The TOE shall provide means to encrypt and decrypt user data and TSF data to maintain confidentiality, integrity and accountability and allow for detection of modification of user data that is transmitted within or outside of the TOE.
O.Access_Control	The TOE shall enable access control on all objects under the control of the TOE (e.g. assets) as well as the TSF and ensure authorized use while preventing unauthorized use.

4.2 Security Objectives for the operational environment

This section describes security objectives that the TOE should address in the operational environment to solve problems with regard to the threats and organizational security policies defined as the security problems. In addition, the security objectives stated herein shall all be derived from the assumptions.

OE.HR-Security	Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy. A written and signed agreement is mandatory as part of contractual obligation for employees, contractors and third party users. Conditions of their employment contract shall state their and the organization's responsibilities for information security. All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures as relevant for their job function. Responsibilities and defined processes shall be in place to ensure an employee's, contractor's or third party user's exit from the organization and that the return of all assets and the removal of all access rights are completed. The following controls shall be fulfilled: [ISO/IEC 27001:2013][8]: A.7 Human resource security
OE.Access_ManagementSystem	Secure Operation of the TOE requires an access-management-system for which an access control policy shall be established, documented and reviewed based on business and information security requirements. Access to systems and applications shall be restricted in accordance with the access control policy. A formal user registration and de-registration process shall be implemented to enable assignment of access rights. The allocation and use of privileged access rights shall be restricted and controlled. Password management systems shall be interactive and shall ensure strong passwords. The following controls shall be applied and fulfilled: - [ISO/IEC 27001:2013]: A.9 Access Control
OE. SecureAreas and Equipment	Critical or sensitive information processing facilities of the IdP shall be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They shall be physically protected from unauthorized access, damage and loss including safeguard supporting facilities, such as the electrical supply and cabling infrastructure. The following controls shall be applied and fulfilled: - [ISO/IEC 27001:2013]: A.11 Physical and environmental security
OE.Configuration and ChangeManagement	In order to ensure the integrity of information processing systems of the IdP, there shall be established strict controls over the implementation of changes. Formal change

	control procedures shall be enforced. They should ensure that security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained. Defined policies and configuration procedures or systems shall be established to keep control of all implemented software as well as the system documentation. The following controls shall be applied and fulfilled: - [ISO/IEC 27001:2013]: A.12.1.2 Change management - [ISO/IEC 27001:2013]: A.12.5 Control of operational software
OE.Malware and Vulnerability Management	The information processing systems of the IdP shall be protected against malicious code and based on malware code detection, security awareness, and appropriate system access and change management controls. Information resources to be used to identify relevant technical vulnerabilities and to maintain awareness have to be defined and made available. When a potential technical vulnerability has been identified, associated risks shall be identified and the following actions shall be taken: - patching the vulnerable systems or - turning off services or capabilities related to the vulnerability - adapting or adding access controls, e.g. firewalls - increased monitoring to detect actual attacks - raising awareness of the vulnerability The following controls shall be applied and fulfilled: - [ISO/IEC 27001:2013]: A.12.2 Protection from malware - [ISO/IEC 27001:2013]: A.12.6 Technical vulnerability management
OE.Logging and Monitoring	The information processing systems of the IdP shall be monitored and information security events shall be recorded. Operator logs and fault logging shall be used to ensure information system problems are identified. Logging facilities and log information should be protected against tampering and unauthorized access. The clocks of all relevant information processing systems shall be synchronized with an accepted Swiss time source to ensure the accuracy of audit logs. The following controls shall be applied and fulfilled: - [ISO/IEC 27001:2013]: A.12.4 Logging and monitoring
OE.Network Security	A policy concerning the use of networks and network services shall exist and implemented. All authentication methods with respect to the security requirements used to control access by remote users shall be defined and documented. Groups of information services, users, and information processing systems in the IdP shall be segregated on networks. Routing controls shall be implemented for networks to ensure that information processing systems connections and information flows do not breach the access control policies. The following controls shall be applied and fulfilled:

	- [ISO/IEC 27001:2013]: A.13.1 Network security management
OE.Identification and IdentityManagement	Secure Operation of the TOE requires the following steps taken beforehand regarding an Identification- and Identity-Management-System: 1. Before a claimant (subscriber) enters into a contractual relationship with a Registration Authority [RA], he shall be informed of the precise terms and conditions by the RA regarding the use of the device/token. 2. The RA shall perform all identity proofing in accordance with the published identity proofing policy and ensure, that subscribers are properly identified and registered. 3. The RA shall accept requests with qualified digital signatures for claimants possessing valid certificates. 4. The RA shall record the signed agreement with the claimant (subscriber). 5. Records with the actions of the RAs and IdPs, shall be stored in corresponding event journals. 6. Communications between the RA and the IdP shall be authenticated and secure. 7. If external RAs are used, a documented process for validating and authorising external registration authorities respecting the information security requirements shall be implemented. 8. The IdP shall provide a policy for managing the identity information lifecycle 9. Processes to maintain the accuracy of the identity information and controls to verify policies, regulations, business requirements and to improve processes shall be established by the IdP. 10. Policies to specify the conditions and procedures to archive identity information shall be established by the IdP. 11. The IdP shall provide policies to specify the conditions and procedures to initiate deletion of identity information. The following controls shall be fulfilled: - [ISO/IEC 29115:2013]: 10.1 Threats to, and controls for, the enrolment phase - [ISO/IEC 24760-2:2015][10]: 6.2 Access policy for identity information - [ISO/IEC 24760-2:2015]: 6.3.1 Policy for identity information life cycle - [ISO/IEC 24760-2:2015]: 6.3.2 Conditions and procedure to maintain identity information - [ISO/IEC 24760-2:2015]: 6.3.5 Identity information quality and compliance - [ISO/IEC 24760-2:2015]: 6.3.6 Archiving information - [ISO/IEC 24760-2:2015]: 6.3.7 Terminating and deleting identity information
OE.Credential Management	1. The IDP shall establish procedures to ensure that the individual who receives the device/token is the same individual who participated in the registration procedure. 2. For issuing a device/token, procedures shall be established, which allow the subscriber to authenticate

	the IdP as the source of the delivered device/token and to check its integrity. 3. The IdP shall revoke a device/token based on a unique identifying attribute in a token or in a credential (e.g. serial number) within a specific time period as defined by a corresponding policy or immediately, when stolen or compromised. An on-line revocation/status checking availability shall be implemented and maintained as well as a web site, on which revocation requests can be submitted in an authenticated manner (security questions, out-of-band notification, etc.) by the claimants. The following controls shall be applied and fulfilled: - [ISO/IEC 29115:2013]: 10.2 Threats to, and controls for, the credential management phase
OE.Operations Security	To ensure correct and secure operations of information processing systems, the IdP shall also implement, maintain and control processes according to the following security controls of the ISO/IEC 27001 Standard: - [ISO/IEC 27001:2013]: A. 12.3 Backup - [ISO/IEC 27001:2013]: A.14.2.1 Secure development policy - [ISO/IEC 27001:2013]: A.14.2.5 Secure system engineering principles - [ISO/IEC 27001:2013]: A.15 Supplier relationships - [ISO/IEC 27001:2013]: A.16 Information security incident management - [ISO/IEC 27001:2013]: A.18.1.3 Protection of records - [ISO/IEC 27001:2013]: A.18.1.4 Privacy and protection of personally identifiable information - [ISO/IEC 27001:2013]: A. 18.2.2 Compliance with security policies and standards
OE.User Security Awareness	1. The RA shall inform the claimant/subscriber through an agreement to submit accurate and complete information to the legal requirements according EPDV, particularly within the registration process. 2. The RA shall inform the claimant/subscriber through an agreement to protect his device/token and furthermore to: - use the device/token only for authentication and in accordance with any other limitations notified to the claimant/subscriber - exercise care to prevent unauthorised use of its device/token 3. The RA shall inform the claimant/subscriber through an agreement and to notify the IdP without any reasonable delay, if any of the following events should occur before the end of the validity period: - the claimant's device/token has been lost, stolen or potentially compromised - control over the claimant's device/token has been lost due to a compromised activation data or other reasons. 4. Claimants shall be aware to communicate revocation requests through protected and authenticated channels with an appropriate user authentication and validation (security questions, out-of-band notification,

	etc.). 5. The RA shall made aware the claimant/subscriber of his responsibilities for maintaining effective access controls, particularly regarding the use of his activation data. 6. The RA shall made aware, that the claimant/subscriber shall keep his computing environment on which the part of the TOE is installed or interacts integer. To achieve this requirement, an anti-virus and personal firewall shall be installed and kept up to date. The entire computing environment shall be updated with the last patches und security updates. The claimant shall be aware and extremely cautious when downloading and/or running executable content such as programs, scripts, macros, add-ons, apps, etc. in order to prevent attacks on the integrity of the computing environment.

Table 6 Security Objectives for the operational environment

4.3 Security Objectives rationale

This chapter describes rationales for the effectiveness of the security objectives stated above for individual parameters of the security problem definition.

4.3.1 Overview

	O.Integrity	O.Confidentiality	O.Availability	O.Accountability	O.Authentication	O.Secure_Communication	O.Cryptographic_Functions	O.Access_Control	OE.HR-Security	OE.Access_ManagementSystem	OE. SecureAreas and Equipment	OE.Configuration and ChangeManagement	OE.Malware and Vulnerability Management	OE.Logging and Monitoring	OE.Network Security	OE.Identification and IdentityManagement	OE.Credential Management	OE.Operations Security	OE.User Security Awareness
P.Audit	X	X		X										X					
P.Crypto	X	X				X	X								X				
P.AccessRights		X			X			X		X									
P.Hardening													X						
T.CompromiseToken/Credential	X	X			X	X	X												X
T.Token/CredentialTheft								X									X		X
T.WebPlatformAttacks						X						X	X	X	X				

	O.Integrity	O.Confidentiality	O.Availability	O.Accountability	O.Authentication	O.Secure_Communication	O.Cryptographic_Functions	O.Access_Control	OE.HR-Security	OE.Access_ManagementSystem	OE. SecureAreas and Equipment	OE.Configuration and ChangeManagement	OE.Malware and Vulnerability Management	OE.Logging and Monitoring	OE.Network Security	OE.Identification and IdentityManagement	OE.Credential Management	OE.Operations Security	OE.User Security Awareness
T.SpoofingAndMasquerading	X	X		X	X	X								X					
T.SessionHijacking	X	X				X									X				
T.Online_Guessing				X	X									X					
T.ReplayAttack				X		X								X					
T.Eavesdropping		X				X									X				
T.Configuration									X			X							
T.DoS			X									X	X		X				
A.Personal																			
A.AcccessManagement																			
A.Physical																			
A.Monitoring														X					
A.Malware													X						
A.Identification																X			
A.Credential Handling																	X		
A.SystemOperation																		X	
A.Client_Platform																			X

Table 7 Rationale for the security objectives

4.3.2 Countering the threats

4.3.2.1 **T.CompromiseToken/Credential**

The threat **T.CompromiseToken/Credential** addresses all compromises of a device/token and their credentials meaning that an attacker gains access to a credential of a registered claimant and impersonates him or her either by credential tampering, credential disclosure, credential duplication, delayed credential revocation or offline guessing.

The protection against this threat is mainly achieved by the security objectives **O.Integrity** by ensuring TSF data integrity, **O.Confidentiality** by ensuring that TSF Data has not been altered in an unauthorized manner, **O.Authentication** by ensuring authenticity and a strong authentication with regard to the client platform, **O.Secure_Communication** by protection of confidentiality and integrity of the received and transmitted user and TSF data and **O.Cryptographic_Functions** by encryption of TSF and User data of the TOE. Furthermore, the security objective for the operational environment **OE.User Security Awareness** shall ensure that the claimant/subscriber is aware of his responsibilities for maintaining effective access controls and obligations with regard to stolen, lost or compromised devices/tokens.

4.3.2.2 **T.Token/CredentialTheft**

The threat **T.Token/CredentialTheft** describes the situation where the token or device has been stolen by an attacker. The attacker then gains access to the TSF data for instance by knowing the activation data and therefore gains access to the TOE.

This threat is countered by the security objectives **O.Access_Control** and the objectives for the TOE environment **OE.Credential Management** and **OE.User Security Awareness**. The objective **O.Access_Control** sets the requirements to prevent unauthorized use by the establishment of access control of all objects under the control of the TOE and the TSF. The objective for the TOE environment **OE.Credential Management** shall ensure secure issuing procedures regarding the device and token and procedures for immediate revocation of stolen or lost devices/tokens.

4.3.2.3 **T.WebPlatformAttacks**

The threat **T.WebPlatformAttacks** addresses incorrect or faulty implementation of application functions related to authentication and session management that allows an attacker to compromise passwords, keys or session tokens by using exploits such as Cross-Site-Scripting, Cross-Site Request Forgery attacks or Injection exploits.

The protection against this threat is achieved by the security objectives **O.Secure_Communication** and the objectives for the TOEs environment OE.Configuration and ChangeManagement, OE.Malware and Vulnerability Management and **OE.Network Security**. The objective OE.Malware and Vulnerability Management ensures that information processing systems are protected against malicious code and that appropriate measures such as malware code detection are in place beside appropriate system access and change management controls. The objective **OE.Network Security** counters this threat by ensuring the security of information in networks and the protection of connected services from unauthorized access. The objective OE.Configuration and ChangeManagement counters this threat by ensuring that security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained.

4.3.2.4 T.SpoofingAndMasquerading

The threat **T.SpoofingAndMasquerading** refers to situations in which an attacker impersonates another entity in order to launch attacks against network hosts, steal data, spread malware or bypass access controls. This may be done by making use of the credential(s) of an entity or otherwise posing as an entity (e.g. by forging a credential).

The protection against this threat is mainly achieved by the security objectives **O.Integrity**, **O.Confidentiality**, **O.Accountability**, **O.Authentication**, **O.Secure_Communication** and the objective for the TOE environment **OE.Logging and Monitoring**. The objectives **O.Integrity** and **O.Confidentiality** shall ensure that TSF data has not been accessed or altered in an unauthorized manner such that the attacker will not be able to masquerade as the owner of the token/device. The objective **O.Accountability** shall ensure that all actions of an entity specifically to establish future investigations and access control monitoring. The objective **O.Authentication** requires any message to be digitally signed and **O.Secure_Communication** that secure communication is supported by the TOE. The objective **OE.Logging and Monitoring** further requires logs and fault logging to ensure information that system problems are identified.

4.3.2.5 T.SessionHijacking

The threat **T.SessionHijacking** addresses the situation where an attacker is able to intercept successful authentication exchange transactions between the claimant and the IdP and to steal or predict valid session data to gain compromised/unauthorized access to the web portal of the service provider.

The protection against this threat is achieved by the security objectives **O.Integrity**, **O.Confidentiality**, **O.Secure_Communication** providing integrity secured, confidential secure channels between the trusted entities. Further it is ensured by the objective for the TOE environment **OE.Network Security**.

4.3.2.6 **T.Online_Guessing**

The threat **T.Online_Guessing** addresses guessing of the token authenticator for instance by using brute force methods based on specific dictionaries.

The protection of this threat is achieved by the objectives **O.Accountability**, ensuring unique tracing of all actions to an entity and **O.Authentication** requiring use of a multi-authentication factor token and supportively the objective for the TOE environment **OE.Logging and Monitoring**.

4.3.2.7 T.ReplayAttack

The threat **T.ReplayAttack** addresses replaying of previously captured messages between the claimant and the IdP in order to authenticate as that claimant.

The protection of this threat is achieved by the security objectives **O.Accountability**, **O.Secure_Communication**, specifically providing nonces or challenges to prove the freshness of the transaction and supportively the objective for the TOE environment **OE.Logging and Monitoring**.

4.3.2.8 **T.Eavesdropping**

The threat **T.Eavesdropping** addresses passively listening to authentication transactions and to capture information that can be used in a subsequent active attack to masquerade as the claimant.

The protection of this threat is achieved by the security objectives **O.Confidentiality**, **O.Secure_Communication**, specifically encrypting all communication appropriately and supportively the objective for the TOE environment **OE.Network Security**.

4.3.2.9 **T.Configuration**

The threat **T.Configuration** addresses exploiting of weaknesses resulting from a wrong configuration setting, incomplete deployment or not up-to-date software of TSF

The protection of this threat is achieved by the security objectives for the TOE environment **OE.HR-Security** and OE.Configuration and ChangeManagement.

4.3.2.10 **T.DoS**

The threat **T.DoS** addresses denial of service attacks focussing on TSF in order to make them unavailable.

The protection of this threat is achieved by the security objectives **O.Availability** and the objectives for the TOE environment OE.Configuration and ChangeManagement, OE.Malware and Vulnerability Management and **OE.Network Security**.

5 Security Requirements

5.1 Overview

The CC allows several operations to be performed on functional components: refinement, selection, assignment, and iteration are defined in chapter C.4 of part 1 of the CC. Each of these operations is used in this PP.

The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is (1) denoted by the word “refinement” in a footnote and the added/changed words are in bold text, or (2) included in text as underlined text and marked by a footnote. In cases where words from a CC requirement were deleted, a separate attachment indicates
10 the words that were removed.

The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as underlined text and the original text of the component is given by a footnote. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are italicized.

The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing as underlined text and the original text of the component is given by a footnote. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are italicized.

20 5.2 Security Functional Requirements for the TOE

This section on security functional requirements (SFR) for the TOE is divided into sub-section following the main security functionality.

5.2.1 Security audit automatic response (FAU_ARP)

FAU_ARP.1 Security alarms

FIA_ARP.1.1	The TSF shall take [one or more of the following actions: audible alarm, SNMP trap, log, email with or without attachments, page to a pager, SMS, visual alert to notify the administrator’s designated personnel and generate an audit record] upon detection of a potential security violation.
Hierarchical to:	No other components.
Dependencies:	**FAU_SAA.1 Potential violation analysis**
Application note:	This requirement applies only for the IdP. Additionally, the security alarms have to be integrated in the monitoring processes of the computing environment of the TOE.

5.2.2 Audit Data Generation (FAU_GEN)

FAU_GEN.1 Audit Generation

FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the not specified[1] level of audit; and

c) *Auditable events listed in the table below:*[2]

Event	Additional Details	Entity
Any event	- Time the event (e.g. request) received	IdP Activity Log
Authenticated successful	- Remote logname/identity - IP address - Claimant ID, if the request was authenticated - First line of request. - Final status. - Size of response in bytes. - Referrer header field	IdP Activity Log
Authenticated unsuccessful	- Remote logname/identity - IP address - First line of request. - Final status. - Size of response in bytes. - Referrer header field	IdP Activity Log
Logged in successful	- Name of the Trusted User, Temporary privileged user - Name and role of the operator	IdP Activity Log
Logged out successful	- Name of the Trusted User, Temporary privileged user - Name and role of the operator	IdP Activity Log
Logon failure	- Name of the Trusted User, Temporary privileged user - Name and role of the operator	IdP Activity Log
Creation of a new claimant	- n/a	IdP Activity Log
Deletion of a claimant	- n/a	IdP Activity Log
Locking of a claimant	- n/a	IdP Activity Log
Successful and rejected	- Name of the subject and	IdP Activity

[1] [selection, choose one of: minimum,basic, detailed, not specified]

[2] [assignment: other specifically defined auditable events]

data and other resource access attempts if applicable	the resources	Log
Changes to system configuration	- Name of the Trusted User - Name and role of the operator	IdP Activity Log
Privileged actions (e.g. password change)	- Name of the Trusted User, Temporary privileged user - Name and role of the operator	IdP Activity Log
Use of system utilities and applications	- Name of the subject and the resources	IdP Activity Log
Alarms raised by the access control system	- Entity	IdP Activity Log
Activation and de-activation of protection systems	- Name of the Trusted User - Name and role of the operator	IdP Activity Log
Incidents	- Source - Number of changes - Analysis – list of suspicious actions - Event Tree: process, file, registry and network events - Timeline: timeline of suspicious actions - Geography: suspected locations of suspicious events - Configuration: host system identification details, running applications, service handles, processes, threads	IdP Incidents Alerts

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP, additional details specified below:[3]

- files accessed (if applicable)
- programs/utilities used
- use of privileged accounts, e.g. supervisor, root, administrator;

[3] [assignment: other audit relevant information]

- system start-up and stop;
- I/O device/connector attachment/detachment;
- failed or rejected user actions;
- failed or rejected actions involving data and other resources;
- access policy violations and notification
- console alerts or messages;
- system log exceptions;
- network management alarms;
- alarms raised by the access control system;
- changes to, or attempts to change, system security settings and controls

Hierarchical to: No other components.

Dependencies: **FPT_STM.1 Reliable time stamps**

Application note: These requirements apply only to the IdP and shall be integrated into the logging and monitoring concept of the computing environment of the TOE.

5.2.3 Security audit analysis (FAU_SAA)

FAU_SAA.1 Potential violation analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of defined auditable events given in the following table[4] known to indicate a potential security violation

b) none[5].

No.	Operation	Potential violation analysis list
1	Authentication	Claimant ID mismatch
2		Authentication attempt with revoked claimant ID
3		Authenticator Token mismatch
4		Authentication error
5		Communication channel not trusted or broken
6		Communication channel with weak encryption
7		Enumerating of access portal
8		DoS-Attack on access portal
9		System alerts
10		Certificate validation and path failures

[4] [assignment: subset of definedauditable events]

[5] [assignment: any other rules]

11		Assertion scheme mismatch
12		Digital signature verification failure

Hierarchical to: No other components.

Dependencies: **FAU_GEN.1 Audit Generation**

Application note: These requirements apply only to the IdP and shall be integrated into the operation security concept of the computing environment of the TOE

5.2.4 Security audit review (FAU_SAR)

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide Trusted Users and/or Temporary privileged users[6] with the capability to read incident reports and the IdP Activity Log[7] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for user to interpret the information.

Hierarchical to: No other components.

Dependencies: **FAU_GEN.1 Audit Generation**

Application note: These requirements apply only on the IdP and shall be integrated into the logging and monitoring concept of the computing environment of the TOE.

5.2.5 Security audit event storage (FAU_STG)

FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_ STG.1.2 The TSF shall be able to prevent[8] unauthorized modifications to the stored audit records in the audit trail.

Hierarchical to: No other components.

Dependencies: **FAU_GEN.1 Audit Generation**

Application note: These requirements apply only to the IdP and shall be integrated into the operation security concept of the computing environment of the TOE

[6] [assignment: authorised users]

[7] [assignment: list of audit information]

[8] [selection, choose one of: prevent, detect]

5.2.6 Management of security attributes (FMT_MSA)

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1	The TSF shall enforce the access control SFP[9] to restrict the ability to query, delete[10] the security attributes Reference of the user credential, Claimant ID, Identification Data[11] to Trusted User[12].
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Application note:	

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1	The TSF shall enforce the access control SFP[13] to provide restrictive[14] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the Security Information Officers[15] to specify alternative initial values to override the default values when an object or information is created.
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Application note:	

[9] [assignment: access control SFP(s), information flow control SFP(s)]

[10] [selection: change_default, query, modify, delete, [assignment: other operations]]

[11] [assignment: list of security attributes]

[12] [assignment: the authorised identified roles]

[13][assignment: access control SFP, information flow control SFP]

[14] [selection, choose one of: restrictive, permissive, [assignment: other property]]

[15] [assignment: the authorised identified roles]

5.2.7 Access control functions (FDP_ACF)

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1	The TSF shall enforce the access control SFP[16] to objects based on the following: User, Trusted User, Temporary privileged users, User data, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes[17].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: Authenticated successful, Authenticated unsuccessful, Logged in successful, Logged out successful, Logon failure, Creation of a new claimant, Deletion of a claimant, Locking of a claimant, Successful and rejected data and other resource access attempts if applicable[18].
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[19].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[20].
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
Application note:	These requirements apply only to the IdP and shall be integrated into the access management system of the computing environment of the TOE.

5.2.8 Access control policy (FDP_ACC)

FDP_ACC.1 Subset access control

FDP_ACC.1.1	The TSF shall enforce the access control SFP[21] on User, Trusted User, Temporary privileged users, User data and operations among subjects and objects

[16] [assignment: access control SFP]

[17] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

[18] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]

[19] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

[20] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

[21] [assignment: access control SFP]

covered by the SFP[22].

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

Application note:

5.2.9 Inter-TSF TSF data consistency (FPT_TDC)

FPT_TDC.1 Inter-TSF basic TSF data consistency

FDP_TDC.1.1 The TSF shall provide the capability to consistently interpret Assertion Data[23] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use OASIS Security Assertion Markup Language (SAML) V2.0[24] when interpreting the TSF data from another trusted IT product.

Hierarchical to: No other components.

Dependencies: No dependencies.

Application note:

5.2.10 Import from outside of the TOE (FDP_ITC)

FDP_ITC.2 Import of user data with security attributes

FDP_ITC.2.1 The TSF shall enforce the access control SFP(s)[25] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: none[26].

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or

[22] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

[23] [assignment: list of TSF data types]

[24] [assignment: list of interpretation rules to be applied by the TSF]

[25] [assignment: access control SFP(s) and/or information flow control SFP(s)]

[26] [assignment: additional importation control rules]

FTP_TRP.1 Trusted path]
FPT_TDC.1 Inter-TSF basic TSF data consistency

Application note:

5.2.11 Cryptographic key management (FCS_CKM)

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [defined by the following standards: ETSI TS 102 176-1 [5], NIST Special Publication 800-133 [6], NIST Special Publication 800-56A, NIST Special Publication 800-56B [7][27] and specified cryptographic key sizes [asymmetric (RSA): 2048 - 4096 Bit, elliptic curve (EC): n ≥ 224, symmetric: ≥ 256 bits, any key sizes of algorithms providing comparable cryptographic strength][28] that meet the following: none[29].

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

Application note:

FCS_CKM.3 Cryptographic key access

FCS_CKM.3.1 The TSF shall perform import the user data with security[30] in accordance with a specified cryptographic key access method import through a secure channel[31] that meets the following: GlobalPlatform Card Specification v.2.3 [14], TLSv1.2 [11], other secure means with defined descriptions[32].

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or

[27] [assignment:cryptographic key generation algorithm]

[28] [assignment: cryptographic key sizes]

[29] [assignment: list of standards]

[30] [assignment: type of cryptographic key access]

[31] [assignment: cryptographic key access method]

[32] [assignment: list of standards]

FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

Application note:

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physically overwriting the keys with random numbers[33] that meets the following: none[34].
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
Application note:	The key destruction method shall be applied on volatile key fragments after a cryptographic operation for authentication purposes. This requirement shall not be applied on libraries for standard communication security applications (e.g. TLS, IPsec).

5.2.12 Cryptographic operation (FCS_COP)

FCS_COP.1(1) Cryptographic operation (Symmetric Key Cryptographic Operation)

FCS_COP.1.1(1)	The TSF shall perform data encryption and decryption operations[35] in accordance with a specified cryptographic algorithm AES[36] with a cryptographic key size 256 bits[37] that meets the following: none[38].
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or

[33] [assignment: cryptographic key destruction method]

[34] [assignment: list of standards]

[35] [assignment: list of cryptographic operations]

[36] [assignment: cryptographic algorithm]

[37] [assignment: cryptographic key sizes]

[38] [assignment: list of standards]

FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1(2) Cryptographic operation (Asymmetric Key operations)

FCS_COP.1.1(2)	The TSF shall perform data encryption and decryption[39] in accordance with a specified cryptographic algorithm RSA, Diffie-Hellman, ElGamal, EC and comparable algorithms[40] and cryptographic key size 2048 - 4096 Bit, n ≥ 224[41] that meet the following: PKCS#1 v1.5, PKCS#1 v2.1[42].
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Application note:	Additionally to the listed cryptographic algorithms, other algorithms are admitted if they provide comparable cryptographic strength.

FCS_COP.1(3) Cryptographic operation (HASH function)

FCS_COP.1.1	The TSF shall perform a HASH operation[43] in accordance with a specified cryptographic algorithm [SHA-256, SHA-512[44]] with a cryptographic key size none[45] that meets the following: FIPS PUB 180-3[46].
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

[39] [assignment: list of cryptographic operations]

[40] [assignment: cryptographic algorithm]

[41] [assignment: cryptographic key sizes]

[42] [assignment: list of standards]

[43] [assignment: list of cryptographic operations]

[44] [assignment: cryptographic algorithm]

[45] [assignment: cryptographic key sizes]

[46] [assignment: list of standards]

FCS_CKM.4 Cryptographic key destruction

Application note:

5.2.13 Authentication failures (FIA_AFL)

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 / IdP	The TSF shall detect when an administrator configurable positive integer within the range of 1 - 20[47] unsuccessful authentication attempts occur related to authentication on the IdP portal or system[48].
FIA_AFL.1.1 / Device/Token	The TSF shall detect when a certain number of[49] unsuccessful authentication attempts occur related to RAD/Activation (5 attempts are allowed) and PUK (authentication (10 attempts are allowed) if provided[50].
FIA_AFL.1.2 / IdP	When the defined number of unsuccessful authentication attempts has been met or surpassed[51], the TSF shall display warning message, stop the function of user authentication for 10 minutes and generate audit data to the event[52].
FIA_AFL.1.2 / Device/Token	When the defined number of unsuccessful authentication attempts has been met or surpassed[53], the TSF shall block the RAD/Activation[54].
Hierarchical to:	No other components.
Dependencies:	**FIA_UID.1 Timing of identification**

Application note:

5.2.14 User authentication (FIA_UAU)

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1	The TSF shall allow all functions allowed to be performed by the non authenticated user according to the defined authentication sequence with corresponding secure authentication process states[55] on behalf of the user to be performed before the user is authenticated.

[47] [selection: [assignment: positive integer number], an administrator configurable positive integer within[assignment: range of acceptable values]]

[48] [assignment: list of authentication events]

[49] [selection: [assignment: positive integer number], an administrator configurable positive integer with-in[assignment: range of acceptable values]]

[50] [assignment: list of authentication events]

[51] [selection: met, surpassed]

[52] [assignment: list of actions]

[53] [selection: met, surpassed]

[54] [assignment: list of actions]

[55] [assignment: list of TSF mediated actions]

FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Hierarchical to:	No other components.
Dependencies:	**FIA_UID.1 Timing of identification**
Application note:	

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Hierarchical to:	FIA_UAU.1 Timing of authentication.
Dependencies:	**FIA_UID.1 Timing of identification**
Application note:	

FIA_UAU.3 Unforgeable authentication

FIA_UAU.3.1	The TSF shall *detect and prevent* use of authentication data that has been forged by any user of the TSF.
FIA_UAU.3.2	The TSF shall detect and prevent[56] use of authentication data that has been copied from any other user of the TSF.
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1	The TSF shall provide at least a 2-factor authentication mechanism using a combination of the following possible authentication components: a) Username and Passphrase or activation data, b) Software/Hardware token verification data, c) Biometric credentials[57] to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the following rules: The TOE first verifies the first one authentication component and then verifies the second one authentication component. If each verification of the two chosen

[56] [selection: detect, prevent]

[57] [assignment: list of multiple authentication mechanisms]

	authentication components has been successfully performed, further TSF-mediated actions are allowed.[58]
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	These SFRs refer to the ability for one of many authentication schemes to be specified, and to the ability for the TSF to authenticate a claimant based on the data passed through any of these schemes. The access web portal of the IdP use an authenticated secure channel to protect authentication/verification data transactions based on TLS 1.2 with at least one server-side certificate authentication.

FIA_UAU.7 Protected authentication feedback

FIA_UAU.7.1	The TSF shall provide only obscured feedback[59] to the user while the authentication is in progress.
Hierarchical to:	No other components.
Dependencies:	**FIA_UID.1 Timing of identification**
Application note:	Obscured feedback implies the TSF does not produce a visible display of any authentication data entered by a user, such as through a keyboard or another entering device (e.g., echo the password). It is acceptable that some indication of progress be returned instead.

5.2.15 User identification (FIA_UID)

FIA_UID.1 Timing of identification

FIA_UID.1.1	The TSF shall allow access to the public web portal of the IdP (restricted to the functions and resources accessible to the subscriber/claimant according to the access control policy assigned for that purpose)[60] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	

[58] [assignment: rules describing how the multiple authentication mechanisms provide authentication]

[59] [assignment: list of feedback]

[60] [assignment: list of TSF-mediated actions]

5.2.16 Management of functions in TSF (FMT_MOF)

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1	The TSF shall restrict the ability to modify the behavior of, enable, disable[61] the functions according to table under FMT_SMF.1 {a ..o}[62] to [Administrators, Operators].
FMT_MOF.1.2	The TSF shall restrict the ability to enable, disable[63] the functions according to table under FMT_SMF.1 {p ..q}[64] to Subscriber/Claimant[65].
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Application note:	

5.2.17 Revocation (FMT_REV)

FMT_REV.1 Revocation

FMT_REV.1.1	The TSF shall restrict the ability to revoke security attributes[66] associated with the users[67] under the control of the TSF to the authorized claimants[68].
FMT_REV.1.2	The TSF shall enforce rules a) The TSF shall revoke immediately the authentication associated with security b) The authorized claimant can revoke the authentication processes activated by the subscriber/claimant and the registration authority[69].
Hierarchical to:	No other components.
Dependencies:	**FMT_SMR.1 Security roles**
Application note:	The IdP has to make available a revocation service using the ocsp protocol

[61] [selection: determine the behaviour

of, disable, enable, modify the behaviour of]

[62] [assignment: list of functions]

[63] [selection: determine the behaviour

of, disable, enable, modify the behaviour of]

[64] [assignment: list of functions]

[65] [assignment: the authorised identified roles]

[66] [assignment: list of security attributes]

[67] [selection: users, subjects, objects, [assignment: other additional resources]]

[68] [assignment: the authorised identified roles]

[69] [assignment: specification of revocation rules]

5.2.18 Security management roles (FMT_SMR)

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

- Administrators,
- Operators,
- Maintenances,
- Claimant,
- and further authorized roles (e.g. supervisors)[70]

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Hierarchical to: No other components.

Dependencies: **FIA_UID.1 Timing of identification**

Application note:

5.2.19 Specification of Management Functions (FMT_SMF)

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [71]

	Management Function	**Entity**
a)	Management of Security Attributes Objects and credentials	IdP Device/Token
b)	Management of Claimant Security Attributes	IdP
c)	Management of Authentication Data	IdP
d)	Management of Audit Trail	IdP
e)	Management of Audited Events	IdP
f)	Management of TOE Access Banner	IdP
g)	Management of Role Definitions, including Role Hierarchies and constraints	IdP
h)	Management of access control and its policy	IdP
i)	Management of TOE configuration data	IdP
j)	Management of cryptographic network protocols	IdP
k)	Management of cryptographic keys	IdP
l)	Management of digital certificates	IdP
m)	Management of identification and authentication policy	IdP
n)	Management of identity	IdP
o)	Management of session services	IdP
p)	Management of device/token	Device/Token
q)	Management Reference authentication data [RAD]	Device/Token

Hierarchical to: No other components.

Dependencies: No dependencies.

[70] [assignment: the authorised identified roles]

[71] [assignment: list of management functions to be provided by the TSF]

Application note:

5.2.20 Replay detection (FPT_RPL)

FPT_RPL.1 Replay detection

FPT_RPL.1.1	The TSF shall detect replay for the following entities: TSF data and security attributes[72].
FPT_RPL.1.2	The TSF shall perform reject data; and audit event[73] when replay is detected.
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	

5.2.21 Time stamps (FPT_STM)

FPT_STM.1 Reliable time stamps

FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	These requirements apply only on the IdP and shall be integrated into the logging and monitoring concept of the computing environment of the TOE.

5.2.22 Limitation on scope of selectable attributes (FTA_LSA)

FTA_LSA.1 Limitation on scope of selectable attributes

FTA_LSA.1.1	The TSF shall restrict the scope of the session security attributes cookies, session-IDs[74], based on user identity, originating location, time of access[75].
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	

5.2.23 Confidentiality of exported TSF data (FTP_ITC)

FTP_ITC.1 Inter-TSF confidentiality transmission

FTP_ITC.1.1	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

[72] [assignment: list of identified entities]

[73] [assignment: list of specific actions]

[74] [assignment: session security attributes]

[75] [assignment: attributes]

FTP_ITC.1.2	The TSF shall permit the TSF[76] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for secure communication of assertions and user data.[77]
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	This is to protect the transmission between the IdP and the associated RP.The TSF shall only use TLS 1.2 (RFC 5246 [11]) or IPsec with IKEv2 (RFC 4301 [12], RFC 7296 [13]).

[76] [selection: the TSF, another trusted IT product]

[77] [assignment: list of functions for which a trusted channel is required].

5.3 Security Requirements Rationale

	O.Integrity	Q.Confidentiality	O.Availability	O.Accontability	O.Authentication	O.Secure_Communication	O.Cryptographic_Functions	O.Access_Control	OE.HR_Security	OE.Acces_ManagementSystem	OE.SecureAreas and Equipment	OE.Configration *and* ChangeManage-	OE.Malware and velnerability Managmenet	OE.Logging and Monitorung	OE.Netswork Security	OE.Identification and IdentityMan-agement	OE.Credential Management	OE.Operations Security	OE.User responsibilities
FAU_ARP.1			X	X															
FAU_GEN.1			X	X															
FAU_SAA.1			X	X															
FAU_SAR.1	X		X	X															
FAU_STG.1	X		X																
FCS_CKM.1							X												
FCS_CKM.3		X			X	X	X	X											
FCS_CKM.4		X					X												
FCS_COP.1		X				X	X												
FDP_ACC.1				X			X	X											
FDP_ACF.1				X				X											
FDP_ITC.2	X	X				X		X											
FIA_AFL.1			X		X		X	X											
FIA_UAU.1				X	X		X	X											
FIA_UAU.2					X			X											
FIA_UAU.3	X				X			X											
FIA_UAU.5					X			X											
FIA_UAU.7		X			X			X											
FIA_UID.1				X	X	X		X											
FMT_MSA.1					X		X	X											

	O.Integrity	Q.Confidentiality	O.Availability	O.Accontability	O.Authentication	O.Secure_Com-munication	O.Crypto-graphic_Func-tions	O.Access_Con-trol	OE.HR_Security	OE.Acces_Man-agementSystem	OE.SecureAreas and Equipment	OE.Configration *and* ChangeManage-	OE.Malware and velnerability Managmenet	OE.Logging and Monitorung	OE.Netswork Security	OE.Identification and IdentityMan-agement	OE.Credential Management	OE.Operations Security	OE.User responsibilities
FMT_MSA.3					X		X	X											
FMT_MOF.1								X											
FMT_REV.1	X		X	X	X			X											
FMT_SMF.1				X	X	X	X	X											
FPT_RPL.1			X	X	X	X													
FTA_LSA.1	X				X	X	(X)	X											
FTP_ITC.1	X	X			X	X	X												
FPT_TDC.1	X			X															
FMT_SMR.1				X	X			X											
FPT_STM.1	X			X															

5.4 Security Assurance Requirements Rationale

The Evaluation Assurance Level for this Protection Profile is **EAL2**.
The reason for choosing assurance level EAL 2 is that this Protection Profile shall provide reasonable assurance for auditing the Electronic Means of Identification in the context of the Federal Act on Electronic Health Records and its regulations.

6 Appendix

6.1 Mapping from English to German/French terms

Term	German	French
Reference community	Stammgemeinschaft	Communauté de référence
Community	Gemeinschaft	Communauté
Healthcare professional	Gesundheitsfachperson	Professionnel de la santé
Electronic identification means	Identifikationsmittel	Moyen d'identification
Regulation on the Electronic Patient Record	Verordnung über das elektronische Patientendossier	Ordonnance sur le dossier électronique du patient
Claimant	Anspruchsberechtigter	Ayant droit
Token	Identifizierungsmerkmal	Caractéristiques d'identification
Credential	Berechtigungsnachweis	Référence d'authentification
Federal Act on Electronic Health Records	Bundesgesetz über das elektronische Patientendossier	Loi fédérale sur le dossier électronique du patient

6.2 Tables

6.3 References

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; Version 3.1, Revision 3, Final, July 2009

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; Version 3.1, Revision 3, Final, July 2009, CCMB-2009-07-002

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; Version 3.1, Revision 3, Final, July 2009, CCMB-2009-07-003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, Revision 3, Final, July 2009, CCMB-2009-07-004

[5] ETSI TS 102 176-1 V2.0.0 (2007-11): Electronic Signatures and Infrastructures (ESI);

Algorithms and Parameters for Secure Electronic Signatures;

Part 1: Hash functions and asymmetric algorithms

[6] NIST Special Publication 800-133: Recommendation for Cryptographic Key Generation

[7] NIST Special Publication 800-56B: Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography

[8] ISO/IEC 27001:2013: Information technology -- Security techniques -- Information security management systems – Requirements

[9] ISO/IEC 29115:2013: Information technology -- Security techniques -- Entity authentication assurance framework

[10] ISO/IEC 24760-2:2015: Information technology -- Security techniques -- A framework for identity management -- Part 2: Reference architecture and requirements

[11] RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2

[12] RFC 4301: Security Architecture for the Internet Protocol

[13] RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2)

[14] GlobalPlatform Card Specification Version 2.3, Public Release October 2015, Document Reference: GPC_SPE_034

6.4 SAML Specification

Note: The specification will be drafted during or subsequently to appraisal.