Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI

SR 816.111.1
Anhang 8 der Verordnung des EDI vom 22. März 2017 über das elektronische Patientendossier

Technische und organisatorische Zertifizierungsvoraussetzungen für Identifikationsmittel und deren Herausgeber (Schutzprofil für Identifikationsmittel)

Technical and organizational Certification Requirements for Electronic Authentication Means and Their Issuers (Protection Profile for Authentication Means)

Ausgabe 2.1: 16. März 2021
Inkrafttreten: 15. April 2021

1 PP Introduction

Das Bundesgesetz über das elektronische Patientendossier (EPDG) verlangt für den Zugriff auf das elektronische Patientendossier (EPD) durch Patientinnen und Patienten sowie durch Gesundheitsfachpersonen eine starke Authentifizierung als Grundlage für eine vertrauenswürdige Identität. Dazu legt das Ausführungsrecht zum EPDG die Anforderungen für die elektronische Identität sowie für den Ausgabeprozess von IDM fest. Um ein hohes Vertrauen in die behauptete Identität von Patientinnen und Patienten sowie Gesundheitsfachpersonen sicherzustellen, müssen die Prozesse für die Registrierung, Verwaltung und Herausgabe von IDM die Anforderungen nach Vertrauensstufe 3 (Level of Assurance 3) der Norm ISO / IEC 29115:2013 erfüllen.

Die technischen und organisatorischen Zertifizierungsvoraussetzungen an die Identifikationsmittel und deren Herausgeber nach Artikel 31 Absatz 2 der Verordnung über das elektronische Patientendossier (EPDV) werden in diesem Schutzprofil konkretisiert. Das Schutzprofil definiert Sicherheitsanforderungen, die von allen Produkten erfüllt werden müssen, welche die elektronische Identifizierung und Authentifizierung für den Zugriff auf die Schweizerische EPD durchführen.

The Swiss Federal Act on Electronic Patient Records (EPRA) requires a strong authentication as the basis for trusted identities for patients and healthcare professionals in order to access the Electronic Patient Record (EPR). To this end, the ordinance for the EPRA (EPRO) sets the requirements concerning electronic identities and the issuing process for Electronic Identification Means (EIM). To assure a high confidence in the claimed identity of patients and healthcare professionals, the related processes for registration, management and issuance of EIM have to comply with the requirements for the Level of Assurance 3 (LoA 3) as defined in ISO/IEC 29115:2013.

The technical and organizational certification requirements concerning EIM and their issuers in accordance with article 31 paragraph 2 of the EPRO, are specified in this Protection Profile. All products performing electronic identification and authentication for the access to the Swiss EPR have to fulfil the requirements specified in this Protection Profile.

1.1 PP Reference

Title:	Protection Profile for Electronic Identification Means and their Authentication Procedures
Version:	2.0
Date:	11.12.2017
Issuer:	Swiss Federal Office of Public Health
Evaluation Assurance Level	The assurance level for this PP is EAL2
CC Version	Version 3.1 Revision 4

1.2 TOE Overview

This protection profile defines the security objectives and requirements for Electronic Identification Means (EIM) including their authentication procedures required to access the Swiss Electronic Patient Record (EPR).

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 Ordinance on the Electronic Patient Record (EPRO) context, namely it provides the following:

- An Identity Provider (IdP) for identification and authentication of registered users.
- Authenticators with at least two authentication factors (e.g. smartcards, apps on handheld devices) carrying private and public credentials.
- An authenticator and a verifier to provide authentication services using an authentication protocol
- An authenticated protected back-channel between IdP and the Relying Party
- Web service / middleware provided by Relying Party (i.e. community portal for patients and healthcare professionals) to exchange HTTP requests and responses as well as assertion references with the IdP redirected through an intermediary via corresponding secure authenticated protected channels.

1.2.2 TOE Usage

The subscriber/claimant possesses and controls an authenticator. Each authenticator holds at least two authentication factors, which are provided and applied by the IdP to authenticate the identity of the claimant. Figure 1 shows system components involved and the figure in chapter 6.2 shows the steps required to authenticate patients and healthcare professionals to grant access to the portal of communities or reference communities.

The TOE is restricted to two components, namely the authenticator and the verifier. The authenticator, which may be part of the claimant's client/computing platform, has at least two authentication factors. The verifier is integrated in the system environment of the IdP.

The Authenticator and the Verifier communicate through an authenticated protected channel using TLS 1.2 or higher with defined sequences of messages that demonstrate that the claimant has possession and control of at least two valid authentication factors to establish his/her identity. Secure authentication protocols also demonstrate to the claimant that he or she is communicating with the intended verifier.

The Registration Authority [RA] is a subsidiary organisation fully integrated in the IdP. All organisations that run a local Registration Authority [LRA] do so on a delegated authority basis from RA. LRAs act as legally independent organisations respecting and applying all relevant policies of the RA.

An Assertion is a statement from an IdP to a Relying Party (RP) that contains identity information about a subscriber/claimant. Assertions shall be signed by the IdP. An Assertion Reference is a data object, created in conjunction with an assertion, which identifies the IdP and includes a pointer to the full assertion held by the IdP. The IdP and the Relying Party communicate through a protected back-channel (IPsec or TLS) to exchange the <ArtifactResolve>-Token and the corresponding <Artifact-Response>-Token as well as the Tokens for the Renewal-Processes according to the WS-Trust standard [29] without using redirects through an intermediary such as a browser (agent of a claimant). Redirects through an intermediary such as a browser can only be accomplished using HTTP requests and responses over a second protected channel using TLS. Since an RP is expecting to get an assertion only from the IdP directly, the attack surface is reduced and it is considerably more difficult to inject assertions directly into the RP.

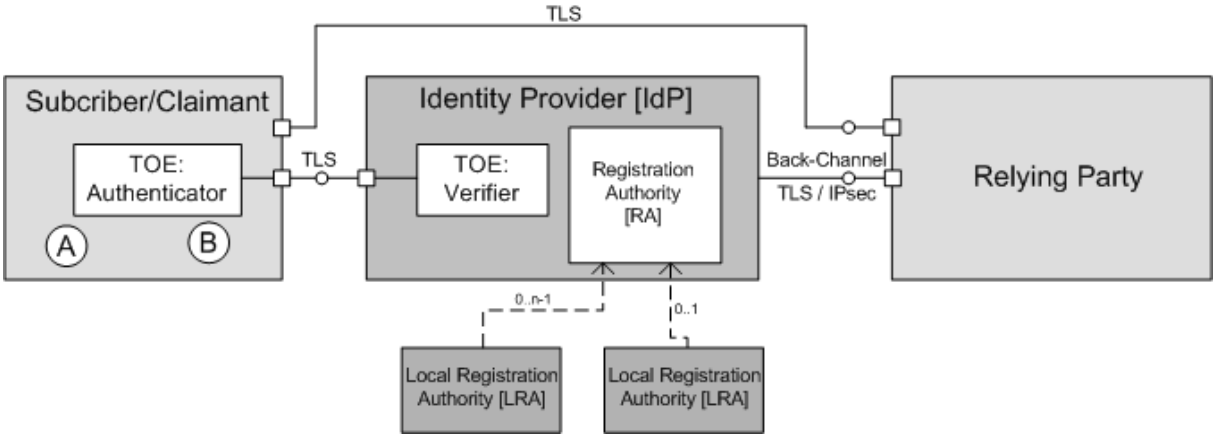

Figure 1 Usage of the TOE

1.3 Operational Environment

EIM have to be compliant with level of assurance 3 (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 EPR.

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 containing the verifier.
- The authenticator is stolen or manipulated by an attacker.

1.5 Assets

The assets to be protected by the TOE are the data objects listed in Table 1. Assets of the TOE are divided into data relating to the TOE Security Function (TSF) and User data as part of the security services provided by the TOE as defined above. The data assets known to the TOE environment, like secret credentials shall be protected by the TOE environment as well.

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

TSF data / User Data	Asset	Description
User data	Authenticator	A device that carries a secret/public credential of an individual user • Disseminated beforehand in a rollout process • Activated with secret only known to the user Note that the device could be of multiple variety (e. g. Chipcard, Handheld-Device, Soft-Token).
User data	Activation secret	Secret to activate the authenticator.
User data	Credential for portal	A credential that is used for specific login into the access portal of the reference community.
User data	User credential on the authenticator	The authenticator stores credential for user authentication in a protected way ensuring confidentiality and integrity.
User data	Reference of user credential	The IdP stores reference of the credential for user authentication in a confidentiality and integrity protecting way.
User data	Authentication protocol messages	A defined sequence of messages between a claimant and a verifier that demonstrates that the claimant has possession and control of one or more valid authenticators to establish his/her identity. Secure authentication protocols also demonstrate to the claimant that he or she is communicating with the intended verifier.
User data	Authenticator output	The output value generated by an authenticator. The ability to generate valid authenticator outputs on demand proves that the claimant possesses and controls the authenticator. Protocol messages sent to the verifier are dependent upon the authenticator output, but they may or may not explicitly contain it.
User data	Identification data	A unique tuple that identifies a user. e.g.Name, date of birth, etc.
TSF data	Cryptographic keys for secure channels	All cryptographic key material used to establish secure channels for communication between parts of the TOE or between the TOE and other trusted components.
TSF data	Claimant ID (EIM Identifier)	A unique ID of the authenticator issued by the IdP to identify the claimant unambiguously.
TSF data	Assertion data	Any SAML assertion defined and generated by the IdP.

1.6 External Entities and Subjects

This protection profile considers the following subjects and external entities:

Table 2 External Entities and Subjects

Entity	Description
User	A patient, a patient's representative, a healthcare professional or an authorized supportive person with access to the EPR.
Trusted Users	Administrators, Operators and Security Information Officers that have privileged access rights to the EIM platform.
Temporary privileged users	Users with temporarily privileged access rights, e.g. developers, support persons or auditors.
Temporary test users	Users with temporary access rights for test purposes only.
Service users	Users without logon, used by system processes.
Attacker	A party who acts with malicious intent to compromise an information system
Relying Party (Service Provider)	Data storage and infrastructure operated by the community 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 authenticators and issues electronic credentials to subscribers. The IdP may encompass Registration Authorities and verifiers that it operates.
Subscriber/Claimant	A user after successful identification and registration.
Client Platform (User Agent)	The platform from which the user requests an identification process at the IdP. Examples: a user's PC or a mobile device with the token.
Service desk	Single point of contact for the management of incidents, problems, configurations and changes. The interface may be a web portal or a telephone number.

2 Conformance Claims

- This PP has been developed using Version 3.1 Revision 4 [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 Part 3 [3] for product certification.

3 Security Problem Definition

The Security Problem Definition describes

- Assumptions on security relevant properties and behaviour 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. 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

Table 3 Assumptions

Assumption	Description
A.Personal	It is assumed that background verification checks on all candidates for employment, employees, 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 acceptable risks. It is assumed, that all employees and contractors understand their information security responsibilities, are aware of information security threats, are authorized and trained according to their roles. Healthcare professionals and patients are assumed to always act with care and according to policies and guidelines of the corresponding part of the TOE. It is assumed, that holders of authenticators and other computing platforms keep secret activation and authentication data confidential, ensuring that it is not disclosed to any other party and that they avoid keeping a record on paper, in a unprotected file or on a handheld device, unless it is securely stored using an approved method.
A.AccessManagement	It is assumed, that access management processes and systems are in place to control the allocation of access rights for authorized users and to prevent unauthorized access to information systems and to physical premises.

Assumption	Description
A.Physical	It is assumed, that the components of the TOE, except for the enrolled authenticator, are operated in a secure area and physically protected against disclosure, manipulations or loss.
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 incidents or 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 information processing systems on the service providing part of the TOE and its computing environment is protected against malware, based on an up-to-date malware detection and correction system service and by information security awareness of the users. 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 the client part of the TOE is installed, is protected against malware, has current patch status of all components and is not used with administrator access rights. It is assumed, that this computing environment is a general home-type environment. This includes having low physical security measures.
A.Identification	It is assumed, that the claimant is carefully identified, well informed and aware of security practices.
A.CredentialHandling	It is assumed, that a mechanism is implemented to ensure that a credential is provided only to the correct entity or an authorized representative. It is assumed, that procedures ensure that a credential or means to generate a credential are only activated, if under the control of the intended entity. The authenticator is protected against unauthorized access with activation secret only known to the subscriber/claimant. In the case of compromise or loss of an authenticator or credential, it is assumed, that the claimant informs immediately the service desk of the IdP through appropriate channels to initiate revocation.

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.

Table 4 Organizational security policies the TOE and its environment shall comply with

Policy	Description
P.Audit	Security relevant events (internal to the TOE or due to the communication flows with the TOE) shall be recorded, stored and reviewed. Audit trail analysis shall be executed in order to hold the authorized users accountable for their actions and to trace attack attempts. At a minimum, the following items should be logged: • date and time • source, network address, terminal identity • user ID • records of successful and rejected system access attempts • changes to system configuration • use of administrative privileges
P.Crypto	State of the art recommended cryptographic functions shall be used to perform all cryptographic operations (e.g. BSI, NIST or other applicable guidance and recommendations). At least the following cryptographic algorithms with keys of length n shall be used: • SHA-2 • AES: n ≥ 256 • RSA: n ≥2048 • ECDSA: n ≥ 224
P.AccessRights	A defined management of access to TOE and network resources shall be established granting identified and authenticated users access to specific resources based on policies and permission levels, assigned to users or user groups. Administrative privileges allow users to make changes on the TOE, including setting up accounts for other users and to change SFR (Security Functional Requirements) specific settings. The allocation and use of such system administration privileges shall be restricted and controlled.
P.Hardening	A defined policy for hardening the TOE shall be established and processes shall be implemented for the systems within the TOE by reducing vulnerabilities. To achieve this, unnecessary software shall be removed, unnecessary services shall disabled or removed, access to resources shall be restricted and controlled, an effective vulnerability and patch management shall be established and maintained.
P.Assertion	SAML-Token has to comply with the specification given in this document. 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 by the IdP using an enhanced signature with a certificate issued by a certified certificate service provider.

Policy	Description
P.TrustedRelyingPartyEndpoint	A trusted relying party endpoint for the secure communication between the TOE and the relying party SHALL be established as defined in this document.

3.3 Threats

This section describes the threats to be averted by the TOE independently or in collaboration with its operational environment. These threats apply to the assets protected by the TOE and the operational environment. The threats described in chapter 10.3 of ISO/IEC 29115:2013 are covered and extended by the following threats.

Table 5 Threats

Threat	Assets/ Security Goals / Adverse Action / Attacker
T.AuthenticatorCompromise	Asset: Credential of the subscribers/claimants authenticator. Security goal: Confidentiality and integrity of the assets. Adverse actions: Exploitation of credential stored on an authenticator An attacker causes an 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 an authenticator 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 by masquerading the rightful claimant (direct use or duplication of the authenticator). An attacker has either direct access to the activation secret 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 authenticator.

Threat	Assets/ Security Goals / Adverse Action / Attacker
	An attacker can capture the activation secret or credentials by sending disguised malware as applications (e.g. keystroke logging software), which can be stored and executed on the authenticator. If the dissemination of revocation information is not timely, it leads to a threat that an authenticator with revoked credentials still being able for authentication until the IdP updates the latest revocation information. Attacker: An attacker alters information during the enrolment process of an authenticator or gains access to a credential of a registered subscriber/claimant and impersonates him or her either by credential tampering, credential disclosure, credential duplication, delayed credential revocation or offline guessing.
T.AuthenticatorTheft	Asset: Credential of the subscribers/claimants authenticator. Security goal: Confidentiality and integrity of the assets. Adverse action: An authenticator which contains credentials is stolen by an attacker. Attacker: If an attacker also knows the activation secret or has direct access to the activation secret by breaking a weak protection mechanism or by applying analytical methods outside the authentication mechanism (offline guessing), favoured by a weak protection mechanism of the authenticator, he can gain authenticated access to 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 accepts 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.

Threat	Assets/ Security Goals / Adverse Action / Attacker
	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 or other included authentication information, to a vulnerable web application. This allows the attacker to force the claimant's browser to generate requests for the vulnerable application, which assumes legitimate requests from the claimant. Injection exploits, such as SQL, OS-Command-Shell, XPATH and LDAP injections 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, resulting in access data access without proper authorization. Web applications frequently redirect and forward users to other pages and websites by using 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 measures on the server for each function to be accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization. <u>Attacker:</u> Not correctly implemented authentication and session management allow an attacker to bypass the authentication methods used by a web application. This enables him to compromise passwords, keys or session tokens, or to exploit other implementation flaws to assume other users identities (unencrypted connections, predictable login credentials, vulnerable 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 three primary types: A) 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 which executes when visiting the target site. B) In Stored XSS, the attacker is able to plant a persistent script into the target website, which will execute when someone visits it. C) With DOM (Document Object Model) Based XSS, no HTTP request is required, since the script is injected by modifying the DOM of the target site in the client side code within the claimant's browser and is then executed. Cross-Site Request Forgery (CSRF) is a web application vulnerability which allows an attacker to force a claimant to unknowingly perform actions while being logged into an application. Attackers commonly use CSRF attacks to target sites such as cloud storage,

Threat	Assets/ Security Goals / Adverse Action / Attacker
	social media, banking and online shopping, because of valuable 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 intending to perform an SQL injection can write a SQL query to replace or concatenate an existing query used by the application, by using specific characters to bypass the query-logic. For an OS command injection, an attacker can inject a shell command by using specific characters to include attacker's commands. Attacks can be tailored according 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 from XML documents, and by injecting malicious input into an XPATH query. This way, an attacker can alter the logic of the query. This attack is known as XPATH injection. Applications, which redirect after a successful authentication to another site by sending a redirect header to the client in an HTTP/HTTPS response, allow an attacker without proper validation a redirection of 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 since 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 or to spread malware. This is achieved by using the credential(s) of an entity or by 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. IP spoofing attacks impersonate machines with access permissions to bypass trust-based network security measures. MAC address spoofing makes a device broadcast and use 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 files in order to reroute a specific domain name to a different IP address. This attack can be used to masquerade a legitimate IdP with an attackers

Threat	Assets/ Security Goals / Adverse Action / Attacker
	malicious IdP or to 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 TSF data. Security goal: The confidentiality and integrity of the assets. Adverse action: An attacker is able to intercept successful authentication transactions between the claimant and the IdP, enabling him 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 codes, trojans, Man-in-the-browser attacks, etc) and Man-in-the-middle attacks. Attacker: An attacker is able to take over an already authenticated session by eavesdropping or by 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 can also log into a vulnerable application, establish 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 authenticator. Attacker: An attacker 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.

Threat	Assets/ Security Goals / Adverse Action / Attacker
	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, then replays it to the IdP to gain access at a later time.
T.Eavesdropping	Asset: Credentials, authentication exchange data and other TSF or 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. 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 (Man-in-the-Middle). Attacker: An attacker captures the transmission of credentials or Session IDs between claimant and IdP.
T.Misconfiguration	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, incomplete hardening or not up-to-date software (libraries, frameworks, and other software modules, almost always running with full privileges) of TSF components of the TOE. Attacker: An unauthenticated or authenticated attacker is able to exploit a weakness by wrong configuration settings, incomplete deployment,

Threat	Assets/ Security Goals / Adverse Action / Attacker
	incomplete hardening or not up-to-date software to gain access to confidential information (user or TSF data).
T.DoS	Asset: The TOE and therefore all assets of the TOE. Security goal: Availability of the TOE and its assets, since a Denial of Service (DoS) attack aims at making the TOE unavailable for the purpose it was designed for. Adverse action: An attacker is able to manipulate network packets, exploit logical or resource handling vulnerabilities or to direct a massive number of network packets to the TOE or its operating environment by using its own infrastructure or infrastructures taken over. Attacker: An (unauthenticated) attacker is able to start an DoS attack onto the external interfaces of the TOE (namely browser interface and web service) with a very large number of requests and may cease it being 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.

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.

Table 6 Security Objectives

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 becoming 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 for access control monitoring.
O.Authentication	Towards the service provider: All messages between IdP and their relying parties shall be digitally signed to guarantee the authenticity and validity shall be time limited. Towards the client platform: The TOE shall provide either an authenticator with two or more authentication factors or a combination of a single-factor authenticator with at least another authenticator transmitted on a separate channel for authentication. The factors shall comply with the requirements of ISO/IEC 29115.
O.SecureCommunication	The TOE shall support secure communication for protection of the confidentiality and the integrity of the user data and TSF

	data received or transmitted. In addition, challenges or timeliness shall be used for freshness of each transaction.
O.CryptographicFunctions	The TOE shall provide means to encrypt and decrypt user data and TSF data to maintain confidentiality, integrity and accountability and to allow for detection of modification of user data that is transmitted within or outside of the TOE.
O.AccessControl	The TOE shall enforce access control on all objects of the TOE (e.g. assets) as well as the TSF, ensuring only 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.

Table 7 Security Objectives for the operational environment

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.AccessManagementSystem	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. SecureAreasAndEquipment	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.ConfigurationAndChangeManagement	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 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.MalwareAndVulnerabilityManagement	The information processing systems of the IdP shall be protected against malicious code, based on malware code detection, security awareness, appropriate system access and change management controls. Information resources 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.LoggingAndMonitoring	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.NetworkSecurity	A policy concerning the use of networks and network services shall exist and shall be implemented. All authentication methods 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 system 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.IdentificationAndIdentityManagement	Secure Operation of the TOE requires the following controls concerning an Identification- and Identity Management System, which is under the control of the Registration Authority (RA). A RA is a subsidiary organisation fully inte-

	grated in the IdP. All organisations that run a Local Registration Authority (LRA) do so on a delegated authority basis from RA. LRAs act as legally independent organisations respecting and applying all relevant policies. LRAs for healthcare professionals, integrated within large trusted healthcare organisations as hospitals, rest homes or communities, can establish more efficient processes to simplify the identity management procedures respecting the required policies and controls. The following controls and processes shall be established and maintained: 1. The IdP and the RA shall provide a policy for managing the identity information lifecycle. 2. The IdP and the RA shall provide policies to specify the conditions and procedures to initiate deletion of identity information. 3. Policies to specify the conditions and procedures to archive identity information shall be established by the IdP and the RA. 4. The IdP and the RA (LRAs) shall establish processes to maintain the accuracy of the identity information and controls to verify policies, regulations, business requirements and to improve procedures. 5. A documented process for validating and authorizing LRAs according to the information security requirements shall be implemented. 6. Communications and proofing transactions between the LRA and the RA shall occur over an authenticated protected and ciphered channel. 7. The RA/LRA shall perform all identity proofing in accordance with the published identity proofing policy and ensure, that subscribers are properly identified and registered based upon authoritative sources. 8. A written practice statement shall specify the particular steps taken to verify identities. 9. All personally identifiable information (PII) collected as part of the enrolment process shall be protected to ensure confidentiality, integrity, and correct assignment of the information source. 10. The RA/LRA requires operators to have undergone a training program to detect potential fraud and to properly perform an identity proofing process as well as a virtual in-person identity proofing session. 11. Before a claimant (subscriber) enters into a contractual relationship with a RA/LRA, he shall be informed of the precise terms and conditions by the RA/LRA regarding the use of the type of authentication factor. 12. The RA/LRA shall record the signed agreement with the subscriber/claimant. 13. The RA/LRA shall provide effective mechanisms for redress of subscriber/claimant complaints or problems arising from the identity proofing. 14. The RA/LRA maintain a record of all steps taken to verify the identity of the subscriber/claimant and shall record the types of identity evidence presented in the proofing process.

	15. The RA shall accept requests from subscriber/ claimant with valid qualified electronic digital signatures. 16. The RA/LRA shall execute the identity proofing process according to [ISO/IEC 29115:2013] “10.1 Threats to, and controls for, the enrolment phase” (see also Appendix 6.1) and integrate the attributes defined in the Swiss Regulation on the Electronic Patient Record. For virtual in-person identity proofing and enrolment transactions, the RA/LRA shall meet the following requirements: a. The RA/LRA shall monitor the entire identity proofing transaction, from which the applicant shall not depart during the identity proofing session (Continuous high-resolution video transmission). b. The RA/LRA shall require all actions taken by the applicant during the enrolment and identity proofing process to be clearly visible to the remote operator. The operator shall direct the applicant as required to remove any doubt in the proofing process. c. The RA/LRA shall require, that all digital verification of evidence be performed by integrated scanners and sensors that are in the entire field of view of the camera and the remote live operator. d. The RA/LRA shall have an operator participate remotely with the applicant for the entirety of the enrolment and identity proofing session. 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 • The IdP shall provide policies to specify the conditions and procedures to archive identity information. Archived identity information SHALL be encrypted to secure the data against unauthorized access. • [ISO/IEC 24760-2:2015]: 6.3.7 Terminating and deleting identity information
OE.CredentialManagement	1. The IdP shall establish procedures to ensure that the individual who receives the authenticator is the same individual who participated in the registration procedure. 2. For issuing an authenticator, procedures shall be established, which allow the subscriber to authenticate the IdP as the source of the delivered authenticator and to check its integrity.

	3. The IdP shall revoke an authenticator based on a unique identifying attribute of the authenticator (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.OperationsSecurity	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 • [ISO/IEC 27001:2013]: A.18.2.3 Technical compliance review
OE.UserSecurityAwareness	1. The RA shall inform the claimant/subscriber through an agreement to submit accurate and complete information to the legal requirements according to EPRO, particularly within the registration process. 2. The RA shall inform the claimant/subscriber through an agreement to protect his authenticator and to ensure: - use the authenticator only for authentication and in accordance with the agreement. - -exercise care to prevent any unauthorised use of its authenticator. 3. The RA shall inform the claimant/subscriber through an agreement and shall 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 authenticator has been lost or stolen

	- or is potentially compromised - or the claimant lost control over its authenticator, for example due to compromised activation secret. 4. Claimants shall 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 make the claimant/subscriber aware of his responsibility for maintaining effective access controls, particularly regarding the use of his activation secret. 6. The RA shall make the claimant/subscriber aware of his responsibility to keep his computing environment (on which the part of the TOE is installed or interacts with) integer. To achieve this requirement, an anti-malware and a 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.

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

Table 8 Rationale for the security objectives

	O.Integrity	O.Confidentiality	O.Availability	O.Accountability	O.Authentication	O.SecureCommunication	O.CryptographicFunctions	O.AccessControl	OE.HR_Security	OE.AccessManagementSystem	OE. SecureAreasAndEquipment	OE.ConfigurationAndChangeManagement	OE.MalwareAndVulnerabilityManagement	OE.LoggingAndMonitoring	OE.NetworkSecurity	OE.IdentificationAndIdentityManagement	OE.CredentialManagement	OE.OperationsSecurity	OE.UserSecurityAwareness
P.Audit	X	X		X										X					
P.Crypto	X	X				X	X								X				
P.AccessRights		X			X			X		X									
P.Hardening													X						
P.Assertion																			
P.TrustedCommunityEndpoint																			
T.AuthenticatorCompro-miseCompromise	X	X			X	X	X												X
T.AuthenticatorTheft								X									X		X

	O.Integrity	O.Confidentiality	O.Availability	O.Accountability	O.Authentication	O.SecureCommunication	O.CryptographicFunctions	O.AccessControl	OE.HR_Security	OE.AccessManagementSystem	OE. SecureAreasAndEquipment	OE.ConfigurationAndChangeManagement	OE.MalwareAndVulnerabilityManagement	OE.LoggingAndMonitoring	OE.NetworkSecurity	OE.IdentificationAndIdentityManagement	OE.CredentialManagement	OE.OperationsSecurity	OE.UserSecurityAwareness
T.WebPlatformAttacks						X						X	X	X	X				
T.SpoofingAndMasquerading	X	X		X	X	X								X					
T.SessionHijacking	X	X				X									X				
T.OnlineGuessing				X	X									X					
T.ReplayAttack				X		X								X					
T.Eavesdropping		X				X									X				
T.Misconfiguration									X			X							
T.DoS			X									X	X		X				
A.Personal																			
A.AcccessManagement																			
A.Physical																			
A.Monitoring														X					
A.Malware													X						
A.ClientPlatform																			
A.Identification																X			
A.CredentialHandling																	X		

4.3.2 Countering the threats

4.3.2.1 T.AuthenticatorCompromise

The threat **T.AuthenticatorCompromise** addresses all compromises of an authenticator 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.SecureCommunication** by protection of confidentiality and integrity of the received and transmitted user and TSF data and **O.CryptographicFunctions** by encryption of TSF and User data of the TOE. Furthermore, the security objective for the operational environment **OE.UserSecurityAwareness** 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 authenticators.

4.3.2.2 T.AuthenticatorTheft

The threat **T.AuthenticatorTheft** describes the situation where the authenticator has been stolen by an attacker. The attacker then gains access to the TSF data for instance by knowing the activation secret and therefore gains access to the TOE.

This threat is countered by the security objectives **O.AccessControl** and the objectives for the TOE environment **OE.CredentialManagement** and **OE.UserSecurityAwareness**. The objective **O.AccessControl** 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.CredentialManagement** shall ensure secure issuing procedures regarding the device and token and procedures for immediate revocation of stolen or lost authenticator.

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.SecureCommunication** and the objectives for the TOEs environment **OE.ConfigurationAndChangeManagement, OE.MalwareAndVulnerabilityManagement** and **OE.NetworkSecurity**. The objective **OE.MalwareAndVulnerabilityManagement** 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.NetworkSecurity** counters this threat by ensuring the security of information in networks and the protection of connected services from unauthorized access. The objective **OE.ConfigurationAndChangeManagement** 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, steals data, spreads malware or bypasses access controls. This may be done by making use of the credential(s) of an entity or otherwise by 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.SecureCommunication** and the objective for the TOE environment **OE.LoggingAndMonitoring**. 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 authenticator. 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.SecureCommunication** that secure communication is supported by the TOE. The objective **OE.LoggingAndMonitoring** 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.SecureCommunication** providing integrity secured, confidential secure channels between the trusted entities. Further it is ensured by the objective for the TOE environment **OE.NetworkSecurity**.

4.3.2.6 T.OnlineGuessing

The threat **T.OnlineGuessing** 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.LoggingAndMonitoring**.

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.SecureCommunication**, specifically providing nonces or challenges to prove the freshness of the transaction and supportively by the objective for the TOE environment **OE.LoggingAndMonitoring**.

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.SecureCommunication**, specifically encrypting all communication appropriately and supportively the objective for the TOE environment **OE.NetworkSecurity**.

4.3.2.9 T.Misconfiguration

The threat **T.Misconfiguration** 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.ConfigurationAndChangeManagement.**

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
10 the TOE environment **OE.ConfigurationAndChangeManagement, OE.MalwareAndVulnerabilityManagement** and **OE.NetworkSecurity**.

5 Security Requirements

5.1 Overview

The CC allow several operations to be performed on functional components: refinement, selection, assignment and iteration as defined in chapter 4.1 of Part 1 of the CC. These operations are 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 as underlined text and marked by a footnote. In cases where words from a CC requirement were deleted, a separate attachment indicates the
10 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 [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 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 The **iteration** operation is used repeat the same component, but applying assignment, selections or refinements in a different way.

5.2 Security Functional Requirements for the TOE

This section on security functional requirements (SFR) for the TOE is structured into sub-sections of security functionalities.

5.2.1 Security audit automatic response (FAU_ARP)

FAU_ARP.1 Security alarms

FAU_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*[1]] 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. The security alarms have to be integrated in the monitoring processes of the computing environment of the TOE.

[1] [assignment: list of actions]

5.2.2 Audit Data Generation (FAU_GEN)

FAU_GEN.1 Audit data 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[2] level of audit; and

c) *Auditable events listed in the table below:*[3]

Event	Additional Details
Any event	- Time of the event (e.g. request)
Authentication successful	- Remote user name / identity - IP address - Claimant ID, if the request was authenticated - First line of request - Final status - Size of response in bytes - Referrer header field
Authentication unsuccessful	- Remote user name / identity - IP address - First line of request - Final status - Size of response in bytes - Referrer header field
Login successful	- Name of the trusted user, temporary privileged user - Name and role of the operator
Logout successful	- Name of the trusted user, temporary privileged user - Name and role of the operator
Logon failure	- Name of the trusted user, temporary privileged user - Name and role of the operator
Creation of a new claimant	- n/a
Deletion of a claimant	- n/a
Locking of a claimant	- n/a
Successful and rejected data and other resource access attempts if applicable	- Name of the subject and the resources

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

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

Changes to system configuration	- Name of the trusted user - Name and role of the operator
Privileged actions (e.g. password change)	- Name of the trusted user, temporary privileged user - Name and role of the operator
Use of system utilities and applications	- Name of the subject and the resources
Alarms raised by the access control system	- Entity
Activation and de-activation of protection systems	- Name of the trusted user - Name and role of the operator
Suspicious activities	- 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

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:[4]

- files accessed (if applicable);
- processes/threads used;
- use of privileged accounts, e.g. supervisor, root, administrator;
- 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 (if applicable)
- system log exceptions (if applicable)
- network management alarms;
- alarms raised by the access control system;
- changes of, or attempts to change, system security settings and controls.

Hierarchical to: No other components.

[4] [assignment: other audit relevant information]

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

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

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 auditable events given in the following table[5] known to indicate a potential security violation

b) none[6].

No.	Operation	Potential violation analysis list
1	Authentication	Claimant ID mismatch
2		Authentication attempt with revoked claimant ID
3		Authenticator mismatch
4		Authentication error
5		Communication channel not trusted or broken
6		Communication channel with weak encryption
7		Enumeration of access portal
8		DoS-Attack on access portal
9		System alert
10		Certificate validation and path failure
11		Assertion scheme mismatch
12		Cryptographic verification failure

Hierarchical to: No other components.

Dependencies: **FAU_GEN.1 Audit data generation**

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

[5] [assignment: subset of defined auditable events]

[6] [assignment: any other rules]

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[7] with the capability to read incident and activity log[8] 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 data generation**
Application note:	These requirements apply only to the verifier and shall be integrated into the logging and monitoring concept of the computing environment of the IdP

FAU_SAR.2 Restricted audit review

FAU_SAR.2.1	The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.
Hierarchical to:	No other components.
Dependencies:	**FAU_SAR.1 Audit review**
Application note:	

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[9] unauthorized modifications to the stored audit records in the audit trail.
Hierarchical to:	No other components.
Dependencies:	**FAU_GEN.1 Audit data 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

[7] [assignment: authorised users]

[8] [assignment: list of audit information]

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

5.2.6 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[10] and specified cryptographic key sizes n [asymmetric (RSA): n: 2048 - 4096 Bit, elliptic curve (EC): n ≥ 224, symmetric: n ≥ 256 bits, any key sizes of algorithms providing comparable cryptographic strength][11] that meet the following:
[5] NIST Special Publication 800-175B, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms,
[6] NIST Special Publication 800-57 Part 1 Revision 4, Recommendation for Key Management, Part 1: General,
[7] NIST Special Publication 800-131A Revision 1, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths,
[18] NIST Special Publication 800-90A Revision 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators,
[19] NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation [12].

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 of user data with security[13] in accordance with a specified cryptographic key access method import through a secure channel[14] that meets the following:
GlobalPlatform Card Specification v.2.3 [14], TLSv1.2 [11] or higher, other equivalent secure means with defined descriptions[15].

Hierarchical to: No other components.

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

[10] [assignment: cryptographic key generation algorithm]

[11] [assignment: cryptographic key sizes]

[12] [assignment: list of standards]

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

[14] [assignment: cryptographic key access method]

[15] [assignment: list of standards]

	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:	

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 logically overwriting the keys with random numbers[16] that meets the following: none[17].
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 does not have to be applied on libraries for standard communication security applications (e.g. TLS, IPsec).

5.2.7 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[18] in accordance with a specified cryptographic algorithm AES[19] and cryptographic key size 256 bits[20] that meets the following: none[21].
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**

[16] [assignment: cryptographic key destruction method]

[17] [assignment: list of standards]

[18] [assignment: list of cryptographic operations]

[19] [assignment: cryptographic algorithm]

[20] [assignment: cryptographic key sizes]

[21] [assignment: list of standards]

Application note: In addition to the listed cryptographic algorithm other algorithms are admitted if they provide comparable cryptographic strength.

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

FCS_COP.1.1(2) The TSF shall perform data encryption and decryption operation[22] in accordance with a specified cryptographic algorithm RSA, Diffie-Hellman, ElGamal, EC and comparable algorithms[23] and cryptographic key sizes n(RSA): 2048 - 4096 Bit, n(EC) ≥ 224[24] that meet the following: [20] PKCS#1 v2.1 or higher[25].

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: In addition 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(3) The TSF shall perform HASH operation[26] in accordance with a specified cryptographic algorithm SHA-256 or higher[27] with a cryptographic key size none[28] that meets the following: none[29].

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:

[22] [assignment: list of cryptographic operations]

[23] [assignment: cryptographic algorithm]

[24] [assignment: cryptographic key sizes]

[25] [assignment: list of standards]

[26] [assignment: list of cryptographic operations]

[27] [assignment: cryptographic algorithm]

[28] [assignment: cryptographic key sizes]

[29] [assignment: list of standards]

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[30] on user, trusted user, temporary privileged users, user data and operations among subjects and objects covered by the SFP[31].
Hierarchical to:	No other components.
Dependencies:	**FDP_ACF.1 Security attribute based access control**
Application note:	None

5.2.9 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[32] 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[33].
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, Logged in successful, Creation of a new claimant, Deletion of a claimant, Locking of a claimant, Successful and rejected data and other resource access attempts if applicable[34].
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[35].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[36].
Hierarchical to:	No other components.
Dependencies:	**FDP_ACC.1 Subset access control**

[30] [assignment: access control SFP]

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

[32] [assignment: access control SFP]

[33] [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]

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

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

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

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.

5.2.10 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[37] 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[38].
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 FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency
Application note:	None

5.2.11 Authentication failures (FIA_AFL)

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 (1 / IdP)	The TSF shall detect when an administrator configurable positive integer within the range of 1 - 20[39] unsuccessful authentication attempts occur related to authentication on the IdP portal or system[40].

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

[38] [assignment: additional importation control rules]

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

[40] [assignment: list of authentication events]

FIA_AFL.1.1 (2 / Authenticator)	The TSF shall detect when more than 5 [41] unsuccessful authentication attempts occur related to Activation secret.[42].
FIA_AFL.1.2 (1 / IdP)	When the defined number of unsuccessful authentication attempts has been met or surpassed[43], the TSF shall display warning message, stop the function of user authentication for 10 minutes and generate audit data to the event[44].
FIA_AFL.1.2 (2 / Authenticator)	When the defined number of unsuccessful authentication attempts has been surpassed[45], the TSF shall block the entry of activation secret.[46].
Hierarchical to:	No other components.
Dependencies:	**FIA_UID.1 Timing of identification**
Application note:	

5.2.12 User authentication (FIA_UAU)

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1	The TSF shall allow all functions allowed by non-authenticated user according to the defined authentication sequence stated by the corresponding secure authentication process[47] on behalf of the user to be performed before the user is authenticated.
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.

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

[42] [assignment: list of authentication events]

[43] [selection: met, surpassed]

[44] [assignment: list of actions]

[45] [selection: met, surpassed]

[46] [assignment: list of actions]

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

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

Application note:

FIA_UAU.3 Unforgeable authentication

FIA_UAU.3.1 The TSF shall detect and prevent[48] use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2 The TSF shall detect and prevent[49] 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 factors:

a) something an entity has (e.g., device signature, passport, hardware device containing a credential, private key)
b) something an entity knows (e.g., password, PIN)
c) something an entity is (e.g., biometric characteristic)
d) something an entity typically does (e.g., behaviour pattern)

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 authentication component and then verifies the second authentication component. If each verification of the two chosen authentication components has been successfully performed, further TSF-mediated actions are allowed.[50]

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 of the TSF to authenticate a claimant based on the data passed through any of these schemes.

The Verifier uses an authenticated secure channel to protect authentication/verification data transactions based at least on TLS 1.2 or higher with at least server-side certificate authentication.

FIA_UAU.6 Re-authenticating

[48] [selection: detect, prevent]

[49] [selection: detect, prevent]

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

FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions: using their primary authentication mechanism or an appropriate subset thereof[51].
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	

FIA_UAU.7 Protected authentication feedback

FIA_UAU.7.1	The TSF shall provide only obscured feedback[52] 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 display any authentication data entered by a user. It is acceptable that some indication of progress to be returned instead.

5.2.13 User identification (FIA_UID)

FIA_UID.1 Timing of identification

FIA_UID.1.1	The TSF shall allow access to the public portal of the verifier within the IdP (restricted to the functions and resources accessible to the subscriber/claimant according to the access control policy assigned for that purpose)[53] 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:	

5.2.14 Management of functions in TSF (FMT_MOF)

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 (1)	The TSF shall restrict the ability to modify the behaviour of[54] the functions enable, disable[55] the functions according to table under FMT_SMF.1 {a ..o}[56] to

[51] [assignment: list of conditions under which re-authentication is required]

[52] [assignment: list of feedback]

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

[54] [selection: determine the behavior of, disable, enable, modify the behaviour of]

[55] [selection: determine the behaviour of, disable, enable, modify the behaviour of]

[56] [assignment: list of functions]

	[Administrators, Operators][57].
FMT_MOF.1.1 (2)	The TSF shall restrict the ability to enable, disable[58] the functions according to table under FMT_SMF.1 {p ..q}[59] to Subscriber/Claimant[60].
Hierarchical to:	No other components.
Dependencies:	**FMT_SMR.1 Security roles** **FMT_SMF.1 Specification of Management Functions**
Application note:	

5.2.15 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[61] to restrict the ability to query, delete[62] the security attributes Reference of the user credential, Claimant ID, Identification Data[63] to Trusted User[64].
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:	None

FMT_MSA.3 Static attribute initialisation

[57] [assignment: the authorised identified roles]

[58] [selection: determine the behaviour of, disable, enable, modify the behaviour of]

[59] [assignment: list of functions]

[60] [assignment: the authorised identified roles]

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

[62] [selection: changedefault, query, modify, delete, [assignment: other operations]]

[63] [assignment: list of security attributes]

[64] [assignment: the authorised identified roles]

FMT_MSA.3.1	The TSF shall enforce the access control SFP[65] to provide restrictive[66] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the Security Information Officers[67] 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:	None

5.2.16 Revocation (FMT_REV)

FMT_REV.1 Revocation

FMT_REV.1.1	The TSF shall restrict the ability to revoke security attributes[68] associated with the users[69] under the control of the TSF to the authorized subscriber/claimant[70].
FMT_REV.1.2	The TSF shall enforce rules a) The TSF shall revoke immediately the authentication associated with security incidents b) The authorized claimant shall revoke the authentication capabilities and means provided by the subscriber/claimant and the registration authority according to the applicable policies[71].
Hierarchical to:	No other components.
Dependencies:	**FMT_SMR.1 Security roles**
Application note:	The IdP has to make available a revocation service using the [21] OCSP protocol

5.2.17 Specification of Management Functions (FMT_SMF)

FMT_SMF.1 Specification of Management Functions

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

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

[67] [assignment: the authorised identified roles]

[68] [assignment: list of security attributes]

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

[70] [assignment: the authorised identified roles]

[71] [assignment: specification of revocation rules]

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [72]

Management Function	Entity
Management of Security Attributes Objects and Credentials	IdP Authenticator
Management of Claimant Security Attributes	IdP
Management of Authentication Data	IdP
Management of Audit Trail	IdP
Management of Audited Events	IdP
Management of TOE Access Banner	IdP
Management of Role Definitions, including Role Hierarchies and constraints	IdP
Management of access control and its policy	IdP
Management of TOE configuration data	IdP
Management of cryptographic network protocols	IdP
Management of cryptographic keys	IdP
Management of digital certificates	IdP
Management of identification and authentication policy	IdP
Management of identity	IdP
Management of session services	IdP
Management of authenticator	Authenticator
Management of Reference Authentication Data [RAD]	Authenticator

Hierarchical to: No other components.

Dependencies: No dependencies.

Application note: None

5.2.18 Security management roles (FMT_SMR)

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

- Administrator,
- Operator,
- Service,
- Claimant,
- and further authorized roles (e.g. supervisors)[73]

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: None

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

[73] [assignment: the authorised identified roles]

5.2.19 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[74].
FPT_RPL.1.2	The TSF shall perform reject data and audit event[75] when replay is detected.
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	

5.2.20 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.

5.2.21 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[76] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2	The TSF shall use [22] OASIS Security Assertion Markup Language (SAML) V2.0[77] when interpreting the TSF data from another trusted IT product.
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	None

5.2.22 Limitation on scope of selectable attributes (FTA_LSA)

FTA_LSA.1 Limitation on scope of selectable attributes

[74] [assignment: list of identified entities]

[75] [assignment: list of specific actions]

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

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

FTA_LSA.1.1	The TSF shall restrict the scope of the session security attributes cookies, session-IDs[78], based on user identity, originating location, time of access[79].
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.
FTP_ITC.1.2	The TSF shall permit the TSF[80] 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.[81]
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]).

[78] [assignment: session security attributes]

[79] [assignment: attributes]

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

[81] [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.SecureCommu-nication	O.Crypto-graphic_Func-	O.AccessControl											
FAU_ARP.1			X	X															
FAU_GEN.1			X	X															
FAU_SAA.1			X	X															
FAU_SAR.1	X		X	X															
FAU_SAR.2	X	X	X	X															
FAU_STG.1	X		X																
FCS_CKM.1	X	X					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	X											
FIA_UAU.6					X		X	X											
FIA_UAU.7		X			X			X											
FIA_UID.1				X	X	X		X											
FMT_MOF.1								X											
FMT_MSA.1					X		X	X											
FMT_MSA.3					X		X	X											
FMT_REV.1	X		X	X	X			X											
FMT_SMF.1				X	X	X	X	X											
FMT_SMR.1				X	X			X											
FPT_RPL.1			X	X	X	X													
FPT_STM.1	X			X															
FPT_TDC.1	X			X															
FTA_LSA.1	X				X	X		X											
FTP_ITC.1	X	X			X	X	X												

The security objective **O.Integrity** addresses unauthorized modifications, ensured by the following security functional requirements:

- FAU_SAR.1 Audit review by enabling interpretation of audit logs by authorized users,
- FAU_SAR.2 Restricted audit review by disabling access to audit logs by unauthorized users,
- FAU_STG.1 Protected audit trail storage by protecting the audit logs against deletion and modification,
- FDP_ITC.2 Import of user data with security attributes by providing import rules,
- FIA_UAU.3 Unforgeable authentication by detective and preventative measures,
- FMT_REV.1 Revocation by restricting revocation of security attributes to authorized users,

- FPT_STM.1 Reliable time stamps by providing reliable time stamps,
- FPT_TDC.1 Inter-TSF basic TSF data consistency by ensuring consistent interpretation of TSF data,
- FTA_LSA.1 Limitation on scope of selectable attributes by restricting security attributes,
- FTP_ITC.1 Inter-TSF trusted channel by providing rules for the trusted channel.

The security objective **O.Confidentiality** addresses unauthorized access, ensured by the following security functional requirements

- FAU_SAR.2 Restricted audit review by disabling access to audit logs by unauthorized users,
- FCS_CKM.1 Cryptographic key generation by providing key generation rules,
- FCS_CKM.3 Cryptographic key access by providing key access rules,
- FCS_CKM.4 Cryptographic key destruction by providing key destruction rules,
- FCS_COP.1 Cryptographic operation by allowing specific operations only,
- FDP_ITC.2 Import of user data with security attributes by providing import rules,
- FIA_UAU.7 Protected authentication feedback by obscuring authentication feedback,
- FTP_ITC.1 Inter-TSF trusted channel by providing rules for the trusted channel.

The security objective **O.Availability** aims at maintaining availability of data, ensured by the following security functional requirements

- FAU_ARP.1 Security alarms by notifying potential security violations,
- FAU_GEN.1 Audit data generation by providing specific audit records,
- FAU_SAA.1 Potential violation analysis by providing analysis rules for audit logs,
- FAU_SAR.1 Audit review by enabling interpretation of audit logs by authorized users,
- FAU_SAR.2 Restricted audit review by disabling access to audit logs by unauthorized users,
- FAU_STG.1 Protected audit trail storage by protecting the audit logs against deletion and modification,
- FIA_AFL.1 Authentication failure handling by providing rules for unsuccessful authentication attempts,
- FMT_REV.1 Revocation by restricting revocation of security attributes to authorized users,
- FPT_RPL.1 Replay detection by detecting and rejecting replay attempts,

The security objective **O.Accountability** aims at accountable entities, ensured by the following security functional requirements

- FAU_ARP.1 Security alarms by notifying potential security violations,
- FAU_GEN.1 Audit data generation by providing specific audit records,
- FAU_SAA.1 Potential violation analysis by providing analysis rules for audit logs,
- FAU_SAR.1 Audit review by enabling interpretation of audit logs by authorized users,
- FAU_SAR.2 Restricted audit review by disabling access to audit logs by unauthorized users,
- FDP_ACC.1 Subset access control by providing subset access rules,
- FDP_ACF.1 Security attribute based access control by providing attribute based access rules,
- FIA_UAU.1 Timing of authentication by restricting functions before authentication,
- FIA_UID.1 Timing of identification by allowing functions before identification,
- FMT_REV.1 Revocation by restricting revocation of security attributes to authorized users,
- FMT_SMF.1 Specification of Management Functions by specifying management functions,
- FMT_SMR.1 Security roles by specifying security roles,
- FPT_RPL.1 Replay detection by detecting and rejecting replay attempts,
- FPT_STM.1 Reliable time stamps by providing reliable time stamps,

- FPT_TDC.1 Inter-TSF basic TSF data consistency by ensuring consistent interpretation of TSF data.

The security objective **O.Authentication** aims at authenticated entities, ensured by the following security functional requirements

- FCS_CKM.3 Cryptographic key access by providing key access rules,
- FIA_AFL.1 Authentication failure handling by providing rules for unsuccessful authentication attempts,
- FIA_UAU.1 Timing of authentication by restricting functions before authentication,
- FIA_UAU.2 User authentication before any action by requiring authentication before any TSF action,
- FIA_UAU.3 Unforgeable authentication by detective and preventative measures,
- FIA_UAU.5 Multiple authentication mechanisms by providing specific 2-factor authentication mechanisms,
- FIA_UAU.6 Re-authenticating by restricting re-authentication,
- FIA_UAU.7 Protected authentication feedback by obscuring authentication feedback,
- FMT_MSA.1 Management of security attributes by restricting access to security attributes,
- FMT_MSA.3 Static attribute initialization by restricting default values of security attributes,
- FMT_REV.1 Revocation by restricting revocation of security attributes to authorized users,
- FMT_SMF.1 Specification of Management Functions by specifying management functions,
- FMT_SMR.1 Security roles by specifying security roles,
- FPT_RPL.1 Replay detection by detecting and rejecting replay attempts,
- FTA_LSA.1 Limitation on scope of selectable attributes by restricting security attributes,
- FTP_ITC.1 Inter-TSF trusted channel by providing rules for the trusted channel.

The security objective **O.SecureCommunication** aims at secure data transfers, ensured by the following security functional requirements

- FCS_CKM.3 Cryptographic key access by providing key access rules,
- FCS_COP.1 Cryptographic operation by allowing specific operations only,
- FDP_ITC.2 Import of user data with security attributes by providing import rules,
- FIA_UID.1 Timing of identification by restricting functions before authentication,
- FMT_SMF.1 Specification of Management Functions by specifying management functions,
- FPT_RPL.1 Replay detection by detecting and rejecting replay attempts,
- FTA_LSA.1 Limitation on scope of selectable attributes by restricting security attributes,
- FTP_ITC.1 Inter-TSF trusted channel by providing rules for the trusted channel.

The security objective **O.CryptographicFunctions** provides cryptographic functions, ensured by the following security functional requirements

- FCS_CKM.1 Cryptographic key generation by providing key generation rules,
- FCS_CKM.3 Cryptographic key access by providing key access rules,
- FCS_CKM.4 Cryptographic key destruction by providing key destruction rules,
- FCS_COP.1 Cryptographic operation by allowing specific operations only,
- FDP_ACC.1 Subset access control by providing subset access rules,
- FIA_AFL.1 Authentication failure handling by providing rules for unsuccessful authentication attempts,
- FIA_UAU.1 Timing of authentication by restricting functions before authentication,
- FIA_UAU.5 Multiple authentication mechanisms by providing specific 2-factor authentication

mechanisms,
- FIA_UAU.6 Re-authenticating by restricting re-authentication,
- FMT_MSA.1 Management of security attributes by restricting access to security attributes,
- FMT_MSA.3 Static attribute initialization by restricting default values of security attributes,
- FMT_SMF.1 Specification of Management Functions by specifying management functions,
- FTP_ITC.1 Inter-TSF trusted channel by providing rules for the trusted channel.

The security objective **O.AccessControl** enforces access to objects, ensured by the following security functional requirements

- FCS_CKM.3 Cryptographic key access by providing key access rules,
- FDP_ACC.1 Subset access control by providing subset access rules,
- FDP_ACF.1 Security attribute based access control by providing attribute based access rules,
- FDP_ITC.2 Import of user data with security attributes by providing import rules,
- FIA_AFL.1 Authentication failure handling by providing rules for unsuccessful authentication attempts,
- FIA_UAU.1 Timing of authentication by restricting functions before authentication,
- FIA_UAU.2 User authentication before any action by requiring authentication before any TSF action,
- FIA_UAU.3 Unforgeable authentication by detective and preventative measures,
- FIA_UAU.5 Multiple authentication mechanisms by providing specific 2-factor authentication mechanisms,
- FIA_UAU.6 Re-authenticating by restricting re-authentication,
- FIA_UID.1 Timing of identification by restricting functions before authentication,
- FMT_MOF.1 Management of security functions behavior by restricting security function management,
- FMT_MSA.1 Management of security attributes by restricting access to security attributes,
- FMT_MSA.3 Static attribute initialization by restricting default values of security attributes,
- FMT_REV.1 Revocation by restricting revocation of security attributes to authorized users,
- FMT_SMF.1 Specification of Management Functions by specifying management functions,
- FMT_SMR.1 Security roles by specifying security roles,
- FTA_LSA.1 Limitation on scope of selectable attributes by restricting security attributes.

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 the Electronic Identification Means in the context of the Federal Act on Electronic Health Records and its regulations.

The EAL2 package contains the following Security Assurance Requirements as described in [3] and [4], while APE instead of ASE components apply to Protection Profiles.

Table 9 Security Assurance Requirements

Assurance Class	Assurance Components
Development	ADV_ARC.1 Security Architecture ADV_FSP.2 Functional specification ADV_TDS.1 TOE design

Assurance Class	Assurance Components
Guidance Documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
Life-cycle Support	ALC_CMC.2 CM capabilities ALC_CMS.2 CM scope ALC_DEL.1 Delivery
Security Target Evaluation	ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition ASE_INT.1 ST introduction ASE_OBJ.2 Security objectives ASE_REQ.2 Security requirements ASE_SPD.1 Security problem definition (ASE_TSS.1 TOE summary specification)
Tests	ATE_COV.1 Coverage ATE_FUN.1 Functional tests ATE_IND.2 Independent testing
Vulnerability Assessment	AVA_VAN.2 Vulnerability analysis

From a security risk perspective the following augmentations are recommended, but not required.

- ATE_DPT.1 Test Depth,
    - which objective is to determine whether the developer has tested the TSF subsystems against the TOE design and the security architecture description,
    - which implies the following additional dependencies:
        - ADV_TDS.2 TOE Design, which is only ADV_TDS.1 in EAL2.
        - ADV_FSP.3 Functional Specification, which is only ADV_FSP.2 in EAL2.
- AVA_VAN.3 Vulnerability analysis,
    - which increases the TOE resistance from basic to enhanced-basic,
    - by additional evidences of sub-activities, as summarized below:
        - a) the ST;
        - b) the functional specification;
        - c) the TOE design;
        - d) the security architecture description;
        - e) the implementation subset selected;
        - f) the guidance documentation;
        - g) the TOE suitable for testing;

- h) information publicly available to support the identification of possible potential vulnerabilities;
- i) the results of the testing of the basic design.

6 Appendix

6.1 Identity Proofing Requirements

The following requirements are based upon ISO/IEC 29115 [9] for LoA3 and NIST SP800-63A [15] for IAL2. They are customized for this domain of electronic health records.

Table 10 Identity Proofing Requirements

Evidence and Process	Requirement
Presence	In-person and virtual in-person
	1. One strong evidence:
Evidence	- Swiss Passport or Swiss Identity Card - Residence Permit for foreigner
	2. Two adequate evidences with the following properties
either	- The issuing source of the evidence confirmed the claimed identity through an identity proofing process. - The issuing process allows reasonably assuming the binding of person and ID. - The evidence contains at least one reference number that uniquely identifies the person to whom it relates.
or	- The evidence contains a photograph, image, or biometric of the person to whom it relates.
or	- Ownership of the evidence can be confirmed through Knowledge Based Verification. - Where the evidence includes digital information, it is protected using cryptographic and/or proprietary methods to ensure the integrity of the information and to enable confirmation of the authenticity of the claimed issuing source. - Where the evidence includes physical security features, it requires proprietary knowledge to be able to reproduce it. - The issued evidence is unexpired.
Verification	Identity information may be self-claimed or self-asserted **In-person:** - Ensure that the entity is in possession of an identification document from at least one policy-compliant authoritative source that bears a photographic image of the holder that matches the appearance of the entity. - Ensure that the presented identification document appears to be a genuine document, properly issued and valid at the time of application. - Verify the accuracy of contact information listed in the identification document by using it to contact the entity. - Corroborate personal information against applicable authoritative information sources and (where possible) sources from other contexts, sufficient to ensure a unique identity. - Verify information previously provided by, or likely to be known only by, the entity.
	Non-person entity [NPE] [e.g. SuisseID with qualified electronic signature]

	- Record information from an authoritative source of identity information, such as common name, description, serial number, MAC address, subject, location, manufacturer, etc. - Trusted hardware (e.g. Smartcard) shall be used at LoA3; - For NPEs already in use, the NPE shall be physically enrolled with a device RA using a LoA3 human-issued credential. Where trusted hardware is used, it should be enabled; - NPEs not yet procured shall be ordered using LoA3 human authentication or digital signature to confirm that the ordering entity is authorized to order the NPE. The manufacturer's RA shall register the NPE, enable any trusted hardware and control the issuance and personalization of the NPE. Trusted hardware will be initialized on connection to the network; - For NPEs other than computers, the binding between the device, the owner, the network or communication carrier and the RA shall be cryptographically secured in a similar manner to a trusted hardware computer - Where software is used, the code shall be digitally signed with a LoA3, human-issued credential before issuance and shall be counter-signed by the RA as proof of acceptance before being taken into use.
Address Confirmation	- Self-asserted address data SHALL NOT be used for confirmation. - Address confirmation may be sent to a mobile telephone (SMS or voice), landline telephone, email, or physical mailing address obtained from records of authoritative sources - An enrolment code consisting of at least 6 random digits SHALL be included in address confirmation. If the enrolment code is also intended to be an authentication factor, it SHALL be reset upon first use. - Enrolment codes sent by means other than physical mail SHALL be valid for a maximum of 10 minutes; those sent to a postal address of record SHALL be valid for a maximum of 10 days. - A notification of proofing SHALL be sent via a different address of record than the destination of the enrolment code.
GLN Confirmation	- IdP which provide the GLN in the identity assertion for healthcare professionals SHALL verify the authorization for practising and the GLN against the cantonal or federal registers.

6.2 Authentication-Sequences

The following requirements are based upon ISO/IEC 29115 [9] and NIST SP800-63A [15]. There are customized for the Swiss EPR.

Assertions need to include an appropriate set of protections to the assertion data itself to prevent attackers from manufacturing valid assertions or re-using captured assertions at disparate RPs. The following requirements shall be considered:

1. Assertions SHALL contain sufficient entropy to prevent an attacker from manufacturing a valid assertion and using it with a target RP.
2. Assertions MAY accomplish the above requirement by use of an embedded nonce, timestamp, assertion identifier, or a combination of these or other techniques.
3. The <AuthnRequest> SHALL be cryptographically signed by the RP and the IdP SHALL validate the signature. The <ArtifactResponse> or <Response> SHALL be cryptographically signed by the IdP and the RP SHALL validate the signature of each such assertion. The signature SHALL either be validated with the public key of a pre-registered X.509 certificate, or the certificate embedded in the assertion. If the public key of the embedded certificate is used, the Relying Party SHALL verify, that the certificate matches the pre-registered one. These

X.509-certificates for an enhanced signature SHALL be issued by a certified certificate service provider. This signature SHALL cover all vital fields of the assertion, including its issuer, audience, subject, expiration, and any unique identifiers.

4. The signature SHALL be asymmetric based on the published public key of the IdP respectively of the RP. The certificate containing the public key SHALL be provisioned out of band at the RP respectively at the IdP (during configuration of the RP or IdP).
5. The IdP MAY encrypt the payload of the assertion using the RP's public key contained in the RP's certificate, which must be issued by a certified certificate service provider.
6. Relying parties SHALL be able to decrypt assertions encrypted with the public key contained in the RP's certificate before processing them.
7. All assertions SHOULD use audience restriction techniques to allow an RP to recognize whether or not it is the intended target of an issued assertion.

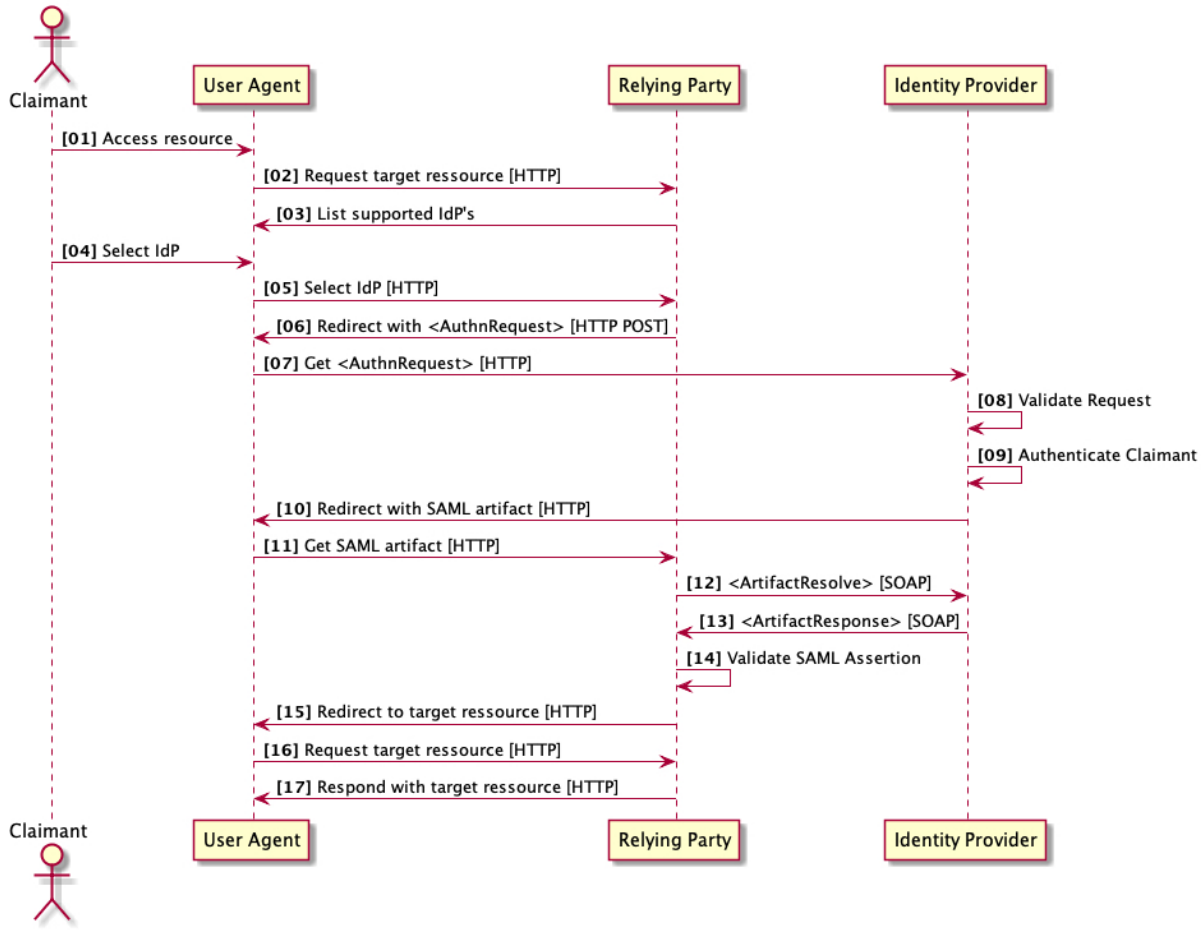

Figure 2: Authentication-Sequence

Table 11 Authentication-Sequence

~~Indirect and direct SP-Initiated~~ **Authentication-Sequence**	
SEQ	**Description**
01,02	The claimant's user agent attempts to access a resource on the relying party. The claimant does not have a valid logon session (i.e. security context) on this site. The Relying Party saves the requested resource URL in local state information.
03	The Relying Party presents the list of supported IdPs to the claimant.
04,05	The claimant selects his dedicated IdP from this list and gives an ok.
06,07	The Relying Party sends an HTML form back to the browser in the HTTP response (HTTP status 200). The HTML form contains a SAML <AuthnRequest> message encoded as the value of a hidden form control named SAMLRequest. Attention: The RelayState mechanism can leak details of the user's activities at the Relying Party to the IdP and so the Relying Party should take care in its implementation to protect the user's privacy.
08	The IdP's Single Sign-On Service determines whether the claimant has an existing logon security context at the IdP that meets the default or requested authentication policy requirements. If not, the IdP interacts with the browser to challenge the claimant to provide valid credentials.
09	The claimant provides valid credentials and a local logon security context is created for that claimant at the IdP.
10,11	The IdP creates an artifact containing the source ID for the relying party site and a reference to the <Response> message (the MessageHandle). The HTTP Artifact binding allows the choice of either HTTP redirection or an HTML form POST as the mechanism to deliver the artifact to the relying party. The figure shows the use of redirection.
12	The RPs Assertion Consumer Service determines the SAML requester by examining the artifact (the exact process depends on the type of artifact) and issues and send a <ArtifactResolve> request containing the artifact to the IdP's Artifact Resolution Service endpoint. This exchange is performed using a synchronous SOAP message exchange over the back-channel.
13	The IdP Artifact Resolution Service extracts the MessageHandle from the artifact and locates the original SAML <Response> message associated with it. This message is then placed inside a SAML <ArtifactResponse> message, which is returned to the Relying Party as a SOAP message over the back-channel.
14…17	The Relying Party verifies the identity assertion retrieved with the <ArtifactResponse>. If the assertion is valid and the claimant is authenticated, the Relying Party returns the requested resource to the claimant's user agent. This MAY require the relying party to present the identity assertion to the EPR platform to authorize the transactions to retrieve the requested resources from the EPR.

Relying Parties MAY renew SAML Identity Assertions for the duration of the IdP idle time of 2 hours after the assertion lifetime has expired without requiring a new authentication of the claimant. To fulfill this requirement, the IdP SHALL operate a web service, which implements a Security Token Service (STS) as defined in the WS-Security Standard [29].

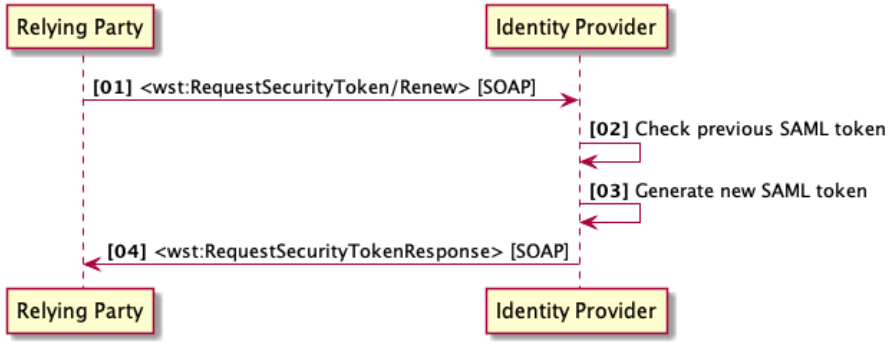

Figure 3 Renewal of a SAML-Assertion

Table 12 Renewal of a SAML-Response-Assertion with new expiration semantics

Renewal of a SAML-Assertion with new expiration semantics	
SEQ	**Description**
01	The Relying Party uses the Identity Assertion of the claimant in a <wst:RequestSecurityToken> request as defined to the WS-Security Standard and sends it to the IdP as SOAP request via the back-channel.
02	The IdP validates the signature of the request and the signature of the assertion conveyed in the request.
03	The IdP generates a new SAML Identity Assertion with a new expiration semantics according to chapter 6.3.
04	The IdP embeds the generated SAML Identity Assertion in the <wst:RequestSecurityTokenResponse> according to the WS-Security Standard. Subsequently the IdP sends this token as SOAP response message over the back-channel.

6.2a Logout Sequence

The following requirements are based upon SAML Profiles 2.0 Chapter 4.4 and are customized for the Swiss EPR.

The <LogoutRequest> and <LogoutResponse> transactions SHALL be protected to prevent attackers from unauthorized use. Identity Provider and Relying Parties shall fulfill the following requirements:

1. The sender (Relying Parties and Identity Provider) shall cryptographically sign the <LogoutRequest> and <LogoutResponse> messages and the receiver SHALL validate the signature with the public key of a pre-registered X.509 certificate.
2. X.509 certificates SHALL be issued by a certified certificate service provider.
3. The sender MAY encrypt the payload of the <LogoutRequest> and <LogoutResponse> using the public key contained in the sender certificate, which must be issued by a certified certificate service provider.
4. Receiver SHALL decrypt encrypted <LogoutRequest> and <LogoutResponse> before processing them.

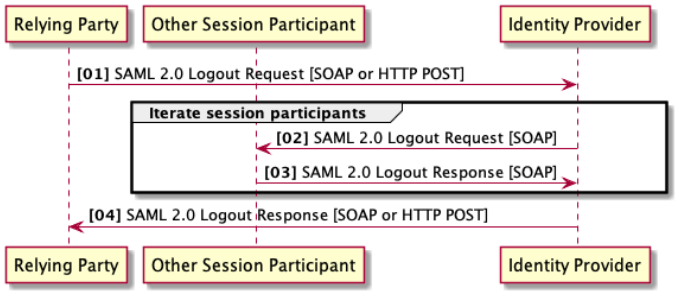

Figure 4 SSO Logout Sequence

Table 13 SSO Logout Sequence

SSO Logout-Sequence-Sequence	
SEQ	**Description**
01	The claimant initiates a logout in the user agent of the Relying Party application. The Relying Party sends a SAML 2 <LogoutRequest> message to the Identity Provider using the SAML 2 http POST or SOAP Binding.
02	The Identity Provider determines the other session participants and sends a <LogoutRequest> message using the SOAP Binding.
03	The other session participants terminate their user session and send a <LogoutResponse> message to the Identity Provider using the SOAP Binding.
04	The Identity Provider terminate the IdP session and responds to the initial <LogoutRequest> with a <LogoutResponse> using the SAML 2 http POST or SOAP Binding.

6.3 SAML Recommendations

The following recommendations are based upon SAML v2 Assertions and Protocols [23], Bindings [24], Profiles [25], Authentication Context [26], Security and Privacy Considerations [27], the OWASP SAML Security Cheat Sheet [28] and NIST SP800-63C [17]. They are customized for this domain of electronic health records and have to be agreed upon by the relevant stakeholders to become requirements.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

Table 14 SAML Recommendations

Items	Recommendations
Compliance	SHALL be according to SAML v2 specifications including errata [22]
Profiles and Bindings	SHALL be A. Login - Direct SP-initiated with Artifact Binding, OR B. Logout - Single Logout Profile (SAML Profiles 2.0 Chapter 4.4) as specified in section 6.2a of this protection profile.
Assertion Validity Period	SAML assertions SHALL only be considered as valid within the time limits specified in the NotBefore and NotOnOrAfter attributes (saml-core-2.0-os [25] chapter 2.5.1.2). Assertions SHALL expire 5 minutes after the assertion has been issued.
Data Types	SHALL be according to W3C XML Schema
ID and ID Reference Values	Any party that assigns an identifier MUST ensure that there is negligible probability that that party or any other party will accidentally assign the same identifier to a different data object. Where a data object declares that it has a particular identifier, there MUST be exactly one such declaration. The Identifiers shall be unique related to the IdP and its own assigned namespaces. The randomly chosen Identifier Values SHALL has a length between 128 and 160 bits. The NameID in the SAML-Response is the Key-ID and SHALL be persistent and confidential outside the IdP-RP-System and never presented neither to the claimant or its agent nor to third-party-systems..
HTTP Artifact Binding	Artifacts SHALL be for one-time-use only SHALL comply with saml-core-2.0-os [23] chapter 3.5 SHALL comply with saml-profiles-2.0-os [25] chapter 5.
Authentication Contexts	SHALL consider saml-authn-context-2.0-os [26]

Items	Recommendations
Request and Response Elements	The RelayState MUST NOT contain any sensitive data. RP SHALL obscure the RelayState in order to protect the user's privacy. Furthermore, the RP SHOULD ensure the integrity of the RelayState. ArtifactResponse SHALL contain with respect to the application context the following attribute set (in accordance with Article 25 EPRO and the saml-core-2.0-os [23] chapter 2.7.3.1) - family name (familyname); - first name (firstname); - gender (gender); - date of birth (dateofbirth); The attribute set MAY contain GLN for healthcare professionals and assistants; Authentication Request SHOULD be signed by the RP; Authentication Response SHALL be signed by the IdP;
Session Index	SAML Assertions SHALL include a <SessionIndex> as element of the <AuthenticationStatement> to enable per session logout requests as defined in Section 4.1.4.2 of the SAML Profiles 2.0 specification. SAML Logout Requests SHALL include at least one <SessionIndex> as defined in Section 4.4.3.1 of the SAML Profiles 2.0 specification.
SAML-Assertion-Definitions	Swiss Federal Office of Public Health SHALL publish the SAML-Assertion-Definitions on a dedicated website

6.4 WS Trust Recommendation

Relying Parties MAY refresh SAML Identity Assertions for the duration of the IdP idle time of 2 hours after the assertion lifetime has expired without requiring a new authentication of the claimant. To fulfill this requirement, the IdP SHALL operate a web service, which implements a Security Token Service (STS) as defined in the WS-Security Standard [29].

Relying Parties MAY use an Identity Assertion of the claimant in a <wst:RequestSecurityToken> request as defined to the WS-Security Standard and send it to the IdP as SOAP request via the back-channel.

The Web Service security header of the SOAP envelope SHALL contain a security timestamp element as described in chapter 10 of the Web Services Security specification. The security timestamp element SHALL have a wsu:Id attribute which shall be used to reference the timestamp element in a XML signature. The security timestamp element SHALL contain a wsu:Created element whose value SHALL be the instant that the renew request is serialized for transmission as described in chapter 10 of the Web Services Security specification. The security timestamp element SHALL contain an wsu:Expires element as described in chapter 10 of the Web Services Security specification.

The Web Service security header of the SOAP envelope SHALL contain a binary token element as described in chapter 6.3 of the Web Services Security specification. The binary token element SHALL

have an encoding type attribute set to EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary". The binary token element SHALL have a value type attribute set to ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3". The binary token element MAY have a wsu:Id attribute.

The Web Service security header of the SOAP envelope SHALL contain a signature element conform to the XML signature specification and described in chapter 8 of the Web Service Security specification. The signature method element SHALL reference a digest algorithm known to resist up to date attacks. Older digest algorithms, doubted to be insecure (for example SHA-1 digest), SHALL not be used. The signature element SHALL contain a key info element with one child element conveying a security token reference conformal to the XML signature specification and described in chapter 7 of the Web Service Security specification. The security token reference element SHALL convey the issuer name and serial number to identify the certificate. The SOAP body element of the request shall have an wsu:Id attribute which is referenced in the key info element of the SOAP security header as described above.

The IdP SHALL

- validate the signature of the request.
- verify the request timestamp, discard any message whose security semantics have passed their expiration and respond with a fault code (wsu:MessageExpired).
- verify the digest algorithm used with the request. The IdP SHALL not accept deprecated digest algorithms, doubted to be insecure (for example SHA-1 digest).
- validate the signature of the previous Identity Assertion conveyed with the <wst:RequestSecurityToken> request.

6.5 Tables

6.6 Figures

6.7 **References**

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; Version 3.1, Revision 5, CCMB-2017-04-001, April 2017.

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; Version 3.1, Revision 5, CCMB-2017-04-002, April 2017.

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; Version 3.1, Revision 5, CCMB-2017-04-003, April 2017.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, Revision 5, CCMB-2017-04-004, April 2017.

[5] NIST Special Publication 800-175B Revision 1, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms, March 2020.

[6] NIST Special Publication 800-57 Part 1 Revision 5, Recommendation for Key Management, Part 1: General, May 2020.

[7] NIST Special Publication 800-131A Revision 2, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, March 2019.

[8] ISO/IEC 27001:2013, Cor. 1:2014 and 2:2015: 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 2.3.1, Public Release March 2018, Document Reference: GPC_SPE_034

[15] DRAFT NIST Special Publication 800-63A, Enrollment and Identity Proofing Requirements, February 2017

[16] DRAFT NIST Special Publication 800-63B, Authentication and Lifecycle Management, February 2017

[17] DRAFT NIST Special Publication 800-63C, Federation and Assertions, February 2017

[18] NIST Special Publication 800-90A Revision 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015

[19] NIST Special Publication 800-133 Revision 2, Recommendation for Cryptographic Key Generation, June 2020.

[20] PKCS #1, RSA Cryptography Standard, v2.2, October 2012

[21] RFC 6960, X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol – OCSP, June 2013 and Errata 5891.

[22] SAML Version 2.0 Errata 05, OASIS Approved Errata, May 2012

[23] Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005: [saml-core-2.0-os]

[24] Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005: [saml-bindings-2.0-os]

[25] Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005: [saml-profiles-2.0-os]

[26] Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005: [saml-authn-context-2.0-os]

[27] Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005: [saml-sec-consider-2.0-os]

[28] https://www.owasp.org/index.php/SAML_Security_Cheat_Sheet

[29] WS-Trust 1.3, A framework for requesting and issuing security tokens, OASIS Standard, March 2007

6.8 Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CA	Certification authority
CC	Common Criteria
CSP	Credential Service Provider
CSRF	Cross Site Request Forgery
DNS	Domain Name System
DOM	Document Object Model
DoS	Denial of Service
EAL	Evaluation Assurance Level
EC	Elliptic Curve
ECDSA	Elliptic Curve Digital Signature Algorithm
EPR	Electronic Patient Record
EIM	Electronic Identification Means
ElGamal	ElGamal encryption system
EPRO	Ordinance on the Electronic Patient Record
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards
EPRA	Federal Act on Electronic Patient Records
GLN	GS1 Global Location Number
HASH	Cryptographic Hash Function
HTTP	Hypertext Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ID	Identifier is either a unique data object or a unique class of objects, which a set of attributes that uniquely describe an entity within a given context.
IdP	Identity Provider

IKE	Internet Key Exchange
IPsec	Internet Protocol Security
LDAP	Lightweight Directory Access Protocol
LoA	Level of Assurance
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
O	Security Objectives for the TOE
OE	Security Objectives for the Operational Environment
OS	Operating System
OSP	Organizational Security Policies
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PP	Protection Profile
RA	Registration Authority
RAD	Reference authentication data
RFC	Request for Comments
RP	Relying Party
RSA	Rivest-Shamir-Adleman Cryptosystem
SAML	Security Assertion Markup Language
SAR	Security Assurance Requirements
SFP	Security Function Policy
SFR	Security Functional Requirements
SHA	Secure Hash Algorithm
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SP	Service Provider
SPD	Security Problem Definition

SQL	Structured Query Language
ST	Security Target
STS	Security Token Service
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
UI	User Interface
XML	Extensible Markup Language
XPATH	XPath is a language for addressing parts of an XML document
XSS	Cross-Site Scripting

6.9 Glossary

Term	Definition
Activation secret	Activation secret, such as a PIN or biometric, may be required to activate the authenticator and permit generation of an authenticator.
Artifact Binding, HTTP Artifact Binding	In the HTTP Artifact binding, the SAML request, the SAML response, or both are transmitted by reference using a small stand-in called an artifact. A separate, synchronous binding, such as the SAML SOAP binding, is used to exchange the artifact for the actual protocol message using the artifact resolution protocol defined in the SAML assertions and protocols specification [SAMLCore]. (Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0)
Assertion	Statement made by an entity without accompanying evidence of its validity. NOTE The meaning of the terms claim and assertion are generally agreed to be somewhat similar but with slightly different meanings. For the purposes of this International Standard, an assertion is considered to be a stronger statement than a claim. (ISO/IEC 29115:2013)

Assertion Data	A data object from a verifier (IdP / CSP) to a Relying Party (RP) that contains identity information about a Claimant/Subscriber. Assertions may also contain verified attributes.
Assets	Entities that the owner of the TOE presumably places value upon. (CC Part 1)
Authentication	Provision of assurance in the identity of an entity. (ISO/IEC 29115:2013)
Authentication Data	Information used to verify the claimed identity of a user. (CC Part 1)
Authentication Factor	Piece of information and/or process used to authenticate or verify the identity of an entity. NOTE Authentication factors are divided into four categories: - something an entity has (e.g., device signature, passport, hardware device containing a credential, private key); - something an entity knows (e.g., password, PIN); - something an entity is (e.g., biometric characteristic); or - something an entity typically does (e.g., behaviour pattern). (ISO/IEC 29115:2013)
Authenticator	Something that the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity. In previous editions of SP 800-63, this was referred to as a token. (NIST SP800-63-3)
Authoritative Source	Repository which is recognized as being an accurate and up-to-date source of information. (ISO/IEC 29115:2013)
Back Channel	Back channel refers to direct communications between two system entities without "redirecting" messages through another system entity such as an HTTP client (e.g. A user agent). See also front channel. (SAML Glossary)
Binding, Protocol Binding	Generically, a specification of the mapping of some given protocol's messages, and perhaps message exchange patterns, onto another protocol, in a concrete fashion. For example, the mapping of the SAML <AuthnRequest> message onto HTTP is one example of a binding. The mapping of that same SAML message onto SOAP is another binding. In the SAML context, each binding is given a name in the pattern "SAML xxx binding".

	(SAML Glossary)
Claimant	A party whose identity is to be verified using an authentication protocol. (NIST SP800-63-2)
Component	Smallest selectable set of elements on which requirements may be based. (CC Part 1)
Credential	Set of data presented as evidence of a claimed or asserted identity and/or entitlements. (ISO/IEC 29115:2013) An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber. (NIST SP800-63-2)
Credential Service Provider	A trusted entity that issues or registers Subscriber tokens and issues electronic credentials to Subscribers. The CSP may encompass Registration Authorities (RAs) and Verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use. (NIST SP800-63-2)
Device	Physical device (e.g. Smartcard Reader, Hand-Held Device (Mobile phone, Pad, Tablet), in which tokens (e.g. Smartcard) are inserted or loaded (Apps), which contain persistent credentials stored in an appropriate secure manner.
Entity	Something that has separate and distinct existence and that can be identified in a context. (ISO/IEC 29115:2013)
Evaluation Assurance Level	Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale that form an assurance package. (CC Part 1)
Federation	This term is used in two senses in SAML: a) The act of establishing a relationship between two entities.

	b) An association comprising any number of service providers and identity providers. (SAML Glossary)
Front Channel	Front channel refers to the “communications channel” that can be effected between two HTTP-speaking servers by employing “HTTP redirect” messages and thus passing messages to each other via a user agent, e.g. a web browser, or any other HTTP client [RFC2616]. See also back channel. (SAML Glossary)
Identifier	One or more attributes that uniquely characterize an entity in a specific context. (ISO/IEC 29115:2013)
Identity	Set of attributes related to an entity. (ISO/IEC 29115:2013)
Identity Provider	A kind of service provider that creates, maintains, and manages identity information for principals and provides principal authentication to other service providers within a federation, such as with web browser profiles. (SAML Glossary)
Inter TSF Transfers	Communicating data between the TOE and the security functionality of other trusted IT products. (CC Part 1)
Internal Communication Channel	Communication channel between separated parts of the TOE. (CC Part 1)
Object	Passive entity in the TOE, that contains or receives information, and upon which subjects perform operations. (CC Part 1)
Operation (on an object)	Specific type of action performed by a subject on an object. (CC Part 1)
Operational environment	Environment in which the TOE is operated. (CC Part 1)
Protection Profile	Implementation-independent statement of security needed for a TOE type.

	(CC Part 1)
Public Credentials	Credentials that describe the binding in a way that does not compromise the token.
Reference authentication data	Reference authentication data (RAD) is securely and persistently stored data within an authenticator to authenticate a user as authorized for a particular role by cognition or by data derived from a user's biometric characteristics
Registration Authority	Trusted actor that establishes and/or vouches for the identity of an entity to a CSP. (ISO/IEC 29115:2013)
Relying Party	Actor that relies on an identity assertion or claim. (ISO/IEC 29115:2013)
SAML Artifact	A small, fixed-size, structured data object pointing to a typically larger, variably-sized SAML protocol message. SAML artifacts are designed to be embedded in URLs and conveyed in HTTP messages, such as HTTP response messages with "3xx Redirection" status codes, and subsequent HTTP GET messages. In this way, a service provider may indirectly, via a user agent, convey a SAML artifact to another provider, who may subsequently dereference the SAML artifact via a direct interaction with the supplying provider, and obtain the SAML protocol message. Various characteristics of the HTTP protocol and user agent implementations provided the impetus for concocting this approach. The HTTP Artifact binding section of [SAMLBind] defines both the SAML Artifact format and the SAML HTTP protocol binding incorporating it. (SAML Glossary)
Secret/Private Credential	Credentials that cannot be disclosed by the IdP or disseminate to the public because the contents can be used to compromise the token.
Security Attribute	Property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used defining the SFRs and whose values are used in enforcing the SFRs. (CC Part 1) Relevant security attributes in this PP include reference of the user credential, ID of the claimant as well as identification data.
Security Function Policy	Set of rules describing specific security behaviour enforced by the TSF and expressible as a set of SFRs. (CC Part 1)

Security Objective	Statement of a intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions. (CC Part 1)
Security Problem	Statement which in a formal manner defines the nature and scope of the security that the TOE is intended to address This statement consists of a combination of: - threats to be countered by the TOE and its operational environment, - the OSPs enforced by the TOE and its operational environment, and - the assumptions that are upheld for the operational environment of the TOE. (CC Part 1)
Subject	Active entity in the TOE that performs operations on objects. (CC Part 1)
Subscriber	A party who has received a credential or token from a CSP. (NIST SP800-63-2)
Target of Evaluation	Set of software, firmware and/or hardware possibly accompanied by guidance. (CC Part 1)
TOE Evaluation	Assessment of a TOE against defined criteria. (CC Part 1)
TOE Security Functionality	Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs. (CC Part 1)
Token	Something that the Claimant possesses and controls (typically an object that contains credentials) that is used to authenticate the Claimant's identity. (NIST SP800-63-2)
Token output / authenticator	The output value generated by a token. The ability to generate valid token authenticators on demand proves that the Claimant possesses and controls the token. Protocol messages sent to the Verifier are dependent upon the token authenticator, but they may or may not explicitly contain it.

Trusted Channel	A means by which a TSF and a remote trusted IT product can communicate with necessary confidence (CC Part 1). In the context of this PP, the transmission between the IdP and the associated RP shall be protected accordingly.
TSF Data	Data for the operation of the TOE upon which the enforcement of the SFR relies. (CC Part 1)
TSF Interface	Means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF, receive data from the TSF and invoke services from the TSF. (CC Part 1)
User Data	Data created by and for the user that does not affect the operation of the TSF. (CC Part 1)
Verifier	Actor that corroborates identity information. (ISO/IEC 29115:2013)