Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI

RS 816.111

Annexe 8 de l'ordonnance du DFI du 22 Mars 2017 sur le dossier électronique du patient

Critères techniques et organisationnels de certification applicables aux moyens d'identification et à leurs éditeurs (profil de protection pour moyens d'identification)

Technical and organizational Certification Requirements for Electronic Authentication Means and Their Issuers

Annexe 8 de l'ODEP-DFI : Critères de certification

Édition 3 : 4 mai 2023

Entrée en vigueur : 1er juin 2023

Table of contents

1 Introduction

La loi fédérale sur le dossier électronique du patient (LDEP) exige qu'un haut degré d'authentification garantisse une identification fiable des patients et des professionnels de la santé pour accéder au dossier électronique du patient (DEP). À cette fin, l'ordonnance sur le dossier électronique du patient (ODEP) fixe les exigences concernant l'identité électronique et le processus de délivrance des moyens d'identification. Pour garantir un haut degré de confiance dans l'identité prétendue d'un patient ou d'un professionnel de la santé, les processus d'enregistrement, d'administration et de délivrance des moyens d'identification doivent satisfaire au niveau de confiance 3 de la norme ISO/IEC 29115:2013 et au niveau d'assurance de l'identité 2 (Identity Assurance Level 2, IAL 2) défini dans la publication spéciale 800-63-3 du NIST.

Les critères techniques et organisationnels de certification applicables aux moyens d'identification et à leurs éditeurs au sens de l'art. 31, al. 2, ODEP sont spécifiés dans les présents critères de certification. Tous les produits effectuant une identification et une authentification électronique pour un accès au DEP suisse doivent remplir les exigences de sécurité spécifiées dans les présents critères de certification. Ces critères définissent les exigences à remplir par tous les produits effectuant une identification et une authentification électroniques pour l'accès au DEP suisse.

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 Electronic Identification Means have to comply with the requirements of Level of Assurance 3 (LOA 3) of ISO / IEC 29115:2013 and Identity Assurance Level 2 (IAL 2) of NIST Special Publication 800-63-3.

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

1.1 Definition of terms

Relying Party: A Relying Party is understood as any actor that relies on an identity claims provided by an Identity Provider for user authentication. In the context of the EPR, Relying Parties are in particular medical information systems and portals for patients and healthcare professionals, which access data and documents from the EPR[1, 2].

Identity Provider: An Identity Provider is understood as a legal entity which manages the Subscriber's primary authentication credentials and issues authenticators and assertions derived from those credentials. Identity Provider typically operate the Verifier and the Credential Service Provider, but may delegate the services to other provider on a contractual basis.

Verifier: A verifier is understood as any Actor that corroborates identity information, by verifying the claimant's identity by verifying the claimant's possession and control of authenticators using an authentication protocol (see fn.1 or 2).

Credential Service Provider: A Credential Service Provider is understood as actor which registers, verifies and provides assertion attributes of Subscriber. The Credential Service Provider typically operates Registration and Local Registration Authorities, but may delegate the services to other provider on a contractual basis (see also fn. 2).

Registration Authority: A Registration Authority is understood as a trusted actor that establishes

1 ISO/IEC 29115:2013: Information technology -- Security techniques -- Entity authentication assurance framework.

2 NIST Special Publication 800-63-3, Digital Identity Guidelines, June 2017 including updates as of February 2020.

and/or vouches for the identity claims of an entity to an Identity Provider. The Registration Authority may be an integral part of an Identity Provider, or it may be independent of an Identity Provider, but has a relationship to the Credential Service Provider (see fn. 1 or 2).

Local Registration Authority: A Local Registration Authority is understood as a legally independent organization that establishes and/or vouches for the identity claims of an entity on behalf of a Registration Authority to an Identity Provider. In the context of the EPR Local Registration Authorities in particular are entities which are integrated in healthcare organizations as hospitals, rest homes or communities. All organizations that run a Local Registration Authority do so on a delegated authority basis from Registration Authority.

Target of Evaluation: The Target of Evaluation is a term used in the Protection Profile (Section 3) which comprises the IT components, services and their operation used by Verifier and Credential Service Provider, including the Registration and Local Registration Authorities.

This document uses the role and state model for enrollment and identity proofing, especially[3]:

Applicant: A user applying for authentication means. The Applicant becomes a Subscriber if identified and in possession of a valid authenticator.

Claimant: A user claiming the identity of a Subscriber using an authentication protocol. The Claimant becomes a Subscriber after successful authentication.

Subscriber: A user who is properly identified and has received authentication means from an Identity Provider, Registration Authorities or Local Registration Authority.

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[4].

1.2 Certification Scope

This document defines the certification criteria for Identity Provider, Registration and Local Registration Authorities for the EPR. The certification criteria cover the requirements for the services towards the user of the EPR (patients, healthcare professionals, assistants and administrators of the communities) and the requirements for the IT Systems used by Identity Provider, Registration and Local Registration Authorities to provide the services towards the users. IT systems acting as Relying Parties are out of scope of the certification.

1.3 Organization of the document

The document is organized as follows:

Section 2 lists the general requirements on Identity Provider, Verifier, Registration and Local Registration Authorities towards the users of the EPR (patients, healthcare professionals, assistants and administrators of the communities) and the Relying Parties.

Section 3 defines the technical and operational requirements for the authenticator, the verifier and the credential service provider operated by the Identity Provider to provide the services towards the users.

Section 4 describes the technical requirements on the protocols to be used by Verifier, Credential Service Provider and the Relying Parties to provide endpoints for secure communication.

[3] NIST Special Publication 800-63-3 B, Authentication and Lifecycle Management, June 2017 including updates as of February 2020.

[4] https://www.rfc-editor.org/rfc/rfc2119 (Accessed 11. Nov. 2022).

2 General Requirements

2.1 Introduction

This section describes the general requirements on Identity Provider, Credential Service Provider, Verifier, Registration and Local Registration Authorities.

2.2 Organizational Requirements

For secure operation of an identification- and identity management system the Identity Provider, Verifier, Registration and Local Registration Authorities SHALL established and maintain the following controls:

a. Registration and Local Registration Authorities SHALL establish processes to maintain the accuracy of the identity information and controls to verify policies, regulations, business requirements and to improve procedures.

b. A documented process for validating and authorizing Local Registration Authorities according to an appropriate Registration Authority Policy with its information security requirements SHALL be established and implemented.

c. The Registration Authorities SHALL ensure high security level processing for all Local Registration Authorities according to the appropriate policy. There SHALL be agreements between the Registration Authority and the Local Registration Authorities to maintain the claimed security level.

d. Registration and Local Registration Authorities SHALL ensure the reliability of the parties involved in the identification and registration process. Particularly, the personnel involved in the non-IT and IT-based actions for Identification and registration have to be trustworthy as defined in the Registration Authority Policy.

e. Registration and Local Registration Authorities SHALL ensure that the identification and registration process is appropriately hardened against eavesdropping and manipulation. Therefore, the Registration Authorities SHALL define within the Terms and Conditions on which way the Local Registration Authorities SHALL transfer the registration data.

f. The data transfer between the Registration and Local Registration Authorities and the Verifier and Credential Service Provider SHALL be hardened against eavesdropping and manipulation, either by using mutual authenticated, protected and ciphered channels for electronic communication (IPsec, mutual TLS 1.2 or higher, TLS 1.2 or higher with message level authentication) or by using postal services.

g. The formal process-flow including the interfaces for requesting the registration and/or providing information by the Applicant SHALL be defined and verified by the Registration Authorities.

h. Training requirements for personnel validating evidence SHALL be based on the policies, guidelines, or requirements of the Registration Authorities.

i. Registration and Local Registration Authorities SHALL require operators to have undergone a training program to detect potential fraud and to properly perform resolution, validation and verification of identity information.

2.3 Authenticator Requirements

Identity Provider SHALL provide an authenticator compliant with Level of Assurance 3 (LOA 3) of ISO/IEC 29115:2013 (fn. 1) and Identity Assurance Level 2 (IAL 2) of NIST Special Publication 800-63-3 B (fn. 3).

The authenticators provided by the Identity Provider SHALL either be a multi-factor authenticator or a combination of two single-factor authenticators.

The following multi-factor authenticator types are permitted:

a. Multi-Factor OTP Device.

b. Multi-Factor Cryptographic Device.

c. Multi-Factor Cryptographic Software.

When a combination of two single-factor authenticators is used, it SHALL include a Memorized Secret authenticator and one possession-based authenticator from the following list:

d. Look-Up Secret.
e. Out-of-Band Device.
f. Single Factor OTP Device.
g. Single-Factor Cryptographic Device.
h. Single-Factor Cryptographic Software.

Biometrics SHALL be used only as part of multi-factor authentication, when combined with a physical authenticator.

The following controls SHALL be applied and fulfilled:

i. ISO/IEC 29115:2013 (fn. 1): 6.3 Level of assurance 3 (LoA3).
j. NIST SP 800-63-3 B (fn. 3): 4.2 Authenticator Assurance Level 2.
k. NIST SP 800-63-3 B (fn. 3): 5. Authenticator and Verifier Requirements.

[NOTE] Authenticators for which known practical attack scenarios exist are not allowed.

[NOTE] Final decisions for applicability of authenticators are with the certification body.

2.4 Issuance Requirements

Registration and Local Registration Authorities SHALL fulfil the following requirements prior to, during and after the registration of the Applicant/Subscriber:

a. The Registration and Local Registration Authorities SHALL maintain a record, including audit logs, of all steps taken to verify the identity of the Applicant and SHALL record the types of identity evidence presented in the proofing process.
b. Collection of personally identifiable information SHALL be limited to the minimum necessary to validate the existence of the claimed identity and associate the claimed identity with the Applicant providing identity evidence for appropriate identity resolution, validation, and verification. This MAY include attributes that correlate identity evidence to authoritative sources.
c. All personally identifiable information collected as part of the enrollment process SHALL be protected by the Registration and Local Registration Authorities to ensure confidentiality, integrity, and correct assignment of the information source.
d. All relevant records in particular personally identifiable information SHALL be protected by the Registration and Local Registration Authorities from loss, destruction, falsification, unauthorized access and unauthorized release.
e. The Registration and Local Registration Authorities SHALL establish processes to maintain the accuracy of the identity information and controls to verify policies, regulations, business requirements and to improve procedures.
f. The Registration and Local Registration Authorities SHALL implement a user interface for Subscriber to access their identity information according to a specified policy.
g. Before an Applicant enters into a contractual relationship with a Registration Authority or Local Registration Authority, the Applicant SHALL be informed of the precise terms and conditions regarding the use of the type of authentication factor.
h. The Terms and Conditions SHALL be delivered by the Registration and Local Registration Authorities and SHALL be accepted by the Applicant.
i. The Registration and Local Registration Authorities SHALL record the agreement with the Subscriber.
j. Registration and Local Registration Authorities SHALL provide effective mechanisms for redress of Applicant/Subscriber complaints or problems arising from the identity proofing.
k. The Registration and Local Registration Authorities SHALL perform all identity proofing in accordance with the published identity proofing policy and ensure, that Applicants/Subscriber are properly identified and registered based upon authoritative sources. This policy SHALL specify the particular steps taken to verify identities and SHALL also include

control information detailing how the Registration and Local Registration Authorities handle proofing errors that result in an Applicant not being successfully enrolled. For example, the number of retries allowed, proofing alternatives (e.g., in-person if remote fails), or fraud countermeasures when anomalies are detected.

l. The Registration and Local Registration Authorities SHALL revoke or destroy credentials/authenticators (including those based on shared secrets) based on a unique identifying attribute (e.g. serial number) within a maximum of 5 years from the date of issuance or immediately, when compromised or stolen.

m. 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 Subscribers. If a Subscriber loses all authenticators or a factor necessary to complete multi-factor authentication and has been identity proofed, the Registration Authority SHALL revoke this authenticator.

n. The Registration and Local Registration Authorities SHALL establish suitable policies for renewal and replacement of credentials. To renew credentials, the Subscriber SHALL authenticate using their existing, unexpired authenticator and credential to request issuance of a new authenticator and credential. If the subscriber fails to request authenticator and credential re-issuance prior to their expiration or revocation, the Subscriber SHALL be required to repeat the enrollment process to obtain a new authenticator and credential.

The following controls SHALL be applied and fulfilled (the symbol "# + Number" refers to respective *Controls for Threats* as defined in ISO/IEC 29115:2013):

o. ISO/IEC 24760-2[5]: 6.3.2: Processes to maintain the accuracy of identity information

p. ISO/IEC 24760-2: 6.3.3: Interface to access identity information

q. ISO/IEC 24760-2: 6.3.5: Identity information quality and compliance

r. ISO/IEC 29115 (fn. 1): 8.2.7: #17

s. ISO/IEC 29115:10.1.2.1: #1

t. ISO/IEC 29115:10.1.2.1: #3

u. ISO/IEC 29115:10.1.2.1: #4 for humans [In-Person, Not-in-person]

v. Biometric template protection in ISO/IEC 24745. [See ISO/IEC 29115:10.2.2.1: #16].

w. ISO/IEC 29115:10.2.2.1: #17, #18

2.5 Identity Proofing Requirements

This section specifies the requirements on identity proofing of users of the EPR (patients, healthcare professionals, assistants and administrators of the communities). For the identity proofing requirements for operational user of the Target of Evaluation, see Section 3.

The following requirements are based upon ISO/IEC 29115 (fn. 1) for LoA3 and NIST SP 800-63-3A for IAL2[6] and customized for the Swiss EPR.

2.5.1 In-person Verification

In-person verification SHALL be according to one of the following schemes (fn. 6):

a. Direct In-Person Verification: Physical interaction with the applicant, supervised by an operator.

b. Supervised Remote In-Person Verification: Remote interaction with the applicant, supervised by an operator (e.g., video identification).

In-person verification SHALL fulfil the following requirements:

c. Verify that the entity is in possession of one of the following evidences:

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

[6] NIST Special Publication 800-63-3 A, Enrollment and Identity Proofing Requirements, June 2017 including updates as of February 2020.

I. Swiss Passport,
II. Swiss Identity Card,
III. Swiss Residence Permit B, C, Ci, G or L for foreigner,
IV. A qualified electronic signature by a recognised certification service provider,
V. Swiss Residence Permit F, N, S in combination with additional evidences (e.g., foreign passport).

d. Verify that the presented identification evidence is genuine. All provided evidence must not be expired at the time of application.
e. Protect all communication for identity proofing against eavesdropping by using a sufficiently secure and undisturbed environment.
f. Protect all documents generated for identity proofing against loss or unauthorized use.

Identity Provider SHALL support all of the evidences listed above. Either, all Registration and Local Registration Authorities SHALL be able to verify the evidences, or SHALL be able to refer a claimant to a Registration or Local Registration Authority which is able to verify the evidence.

2.5.2 Supervised Remote In-person Verification

For supervised remote in-person verification the Registration and Local Registration Authorities SHALL meet the following requirements:

The Registration Authority or Local Registration Authority SHALL:

a. Monitor the entire verification session, from which the Applicant SHALL NOT depart during the session (Continuous high-resolution video transmission).
b. Require all actions taken by the Applicant during the enrollment and in-person verification process to be clearly visible to the remote operator. The operator SHALL direct the Applicant as required to remove any doubt in the in-person verification process.
c. Require, that all digital verification of evidence is performed by integrated scanners and sensors that are in the entire field of view of the camera and the operator.
d. Have an operator participate remotely with the Applicant for the entirety of the in-person verification session.
e. Require operators to have undergone a training program to detect potential fraud and to properly perform a supervised remote in-person verification session.
f. Apply measures against physical and logical manipulation for the supervised remote in-person verification system depending of the environment in which it is located.
g. Ensure that electronic systems used for remote In-person verification communicate via protected channels.
h. Require that identification by video transmission is based on a procedure for which no known attacks exist.

2.5.3 Not-in-Person evidence verification

Not-in-person verification SHALL fulfill the following requirements:

a. Verify that the entity is in possession of a qualified electronic certificate as defined in “Bundesgesetz über die elektronische Signatur, ZertES”.
b. Verify that the presented identification evidence is genuine and valid at the time of application.

2.5.4 Address confirmation

Address confirmation SHALL fulfil the following requirements:

a. The Registration Authority SHALL send a notification of proofing to a confirmed address of record.
b. The Registration Authority SHALL provide a valid enrollment code directly to the Subscriber or send to a confirmed and validated address of record for the Applicant if binding to an authenticator will occur at a later time.
c. The Applicant SHALL present a valid enrollment code to complete the identity proofing process.
d. If the enrollment code is also intended to be an authentication factor, it SHALL be reset upon first use.
e. Enrollment codes SHALL have the following maximum validities:
    I. 10 days, when sent to a postal address.
    II. 10 minutes, when sent to a telephone (SMS or voice).
    III. 1 hour, when sent to an email address.
f. The Registration Authority SHALL ensure the enrollment code and notification of proofing are sent out-of-band to different addresses of record.

2.5.5 GLN confirmation

Identity Provider which provide the optional GLN in the identity assertion for healthcare professionals and assistants SHALL verify the authorization for practicing and the GLN against the cantonal or federal registers.

3 Protection Profile

3.1 Protection Profile Introduction

This section specifies the technical certification requirements concerning Electronic Identification Means (EIM) and their issuers in a Commons Criteria Protection Profile scheme.

3.1.1 Target of Evaluation Definition

This protection profile defines the security objectives and requirements for EIM required to access the Swiss EPR.

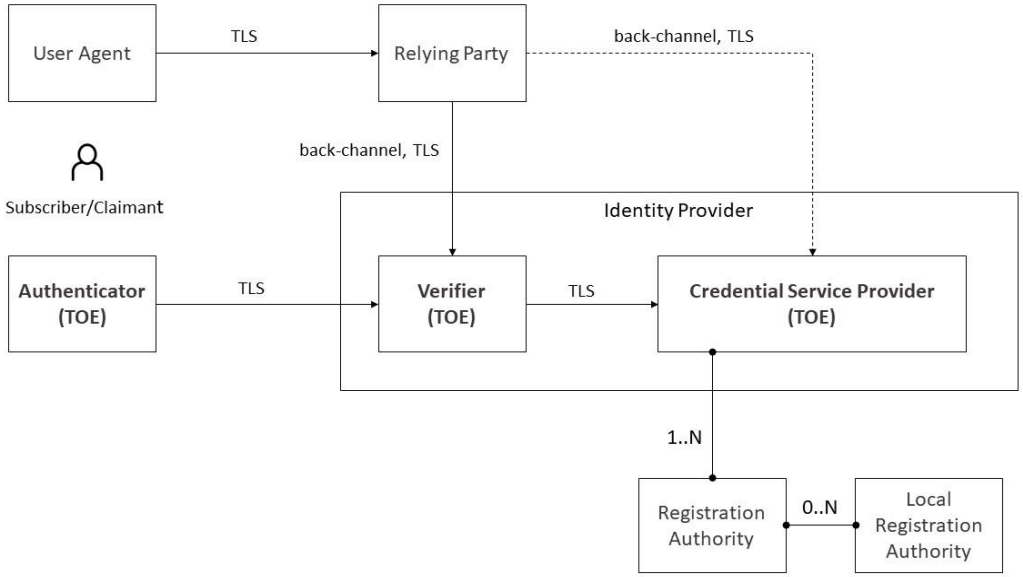

Figure 1: Target of Evaluation and connected systems

The Target of Evaluation comprises the following artefacts and services provided by the Identity Provider:

a. the authenticator,
b. the verifier,
c. the credential service provider.

3.1.2 Operational Environment

Electronic Identification Means SHALL be compliant to Level of Assurance 3 (LOA 3) of ISO/IEC 29115:2013 (see fn. 1) and Identity Assurance Level 2 (IAL 2) of NIST Special Publication 800-63-3 (see fn. 2). It is assumed that Electronic Identification Means meet all necessary requirements related to enrolment, credential management and entity authentication defined for Level of Assurance 3 (LOA 3) in ISO/IEC 29115:2013 and Identity Assurance Level 2 (IAL 2) in NIST Special Publication 800-63-3 B (see fn. 3).

3.1.3 Physical Protection

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

a. Access to the Target of Evaluation infrastructure is not sufficiently restricted and the attacker gains unauthorized access to the server environment containing the verifier.
b. The authenticator is stolen or manipulated by an attacker.

3.1.4 Assets

The assets to be protected by the Target of Evaluation are the data objects listed in **Fehler! Verweisquelle konnte nicht gefunden werden.Fehler! Verweisquelle konnte nicht gefunden werden.**.

The assets are divided into data relating to the Target of Evaluation Security Function (TSF) and User data as part of the security services provided by the Target of Evaluation as fdefined above.

The data assets known to the Target of Evaluation environment, like secret credentials SHALL be protected by the Target of Evaluation environment as well.

TSF data / User Data	Asset	Description
User data	Authenticator	Something the Claimant possesses and controls (typically a cryptographic device or password) that is used to authenticate the Claimant's identity: - 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. Chip card, Handheld-Device, Soft-Token).
User Data	Authentication Factor	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) - Something an entity typically does (e.g., behavior pattern)
User Data	Memorized Secret	A type of authenticator comprised of a character string intended to be memorized or memorable by the Subscriber, permitting the Subscriber to demonstrate something they know as part of an authentication process.
User Data	Authenticator Secret	The secret value contained within an authenticator
User data	Activation secret	Secret to activate the authenticator.
User Data	Credential	An object or data structure that authoritatively binds an identity via an identifier or identifiers and (optionally) additional attributes, to at least one authenticator possessed and controlled by a Subscriber for authentication in a protected way ensuring confidentiality and integrity.
User Data	Public Credentials	Credentials that describe the binding in a way that does not compromise the authenticator.
User Data	Private Credentials	Credentials that cannot be disclosed by the Credential Service Provider because the contents can be used to compromise the authenticator.
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 Verifier or Credential Service Provider stores reference of the credential for user authentication in a confidentiality and integrity protecting way.
User data	Authentication Protocol Messages	A 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.
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 Target of Evaluation or between the Target of Evaluation and other trusted components.
TSF data	Claimant ID	A unique ID of the authenticator issued by the Credential Service Provider to identify the Claimant unambiguously.

TSF data / User Data	Asset	Description
TSF data	Verifier	An entity that verifies the Claimant's identity by verifying the Claimant's possession and control of authenticators using an authentication protocol. To do this, the verifier may also need to validate credentials that link the authenticators to the Subscriber's identifier and check their status.
TSF data	Assertion data	Assertion defined and generated by the Credential Service Provider and presented to Relying Parties that contains information about a Subscriber.
TSF data	Assertion Reference	A data object, created in conjunction with an assertion, which includes a pointer to the full assertion held by the Verifier or Credential Service Provider.

Table 1: Assets of the Target of Evaluation divided into TSF and User data

3.1.5 External Entities and Subjects

This protection profile considers the following subjects and external entities:

Entity	Description
User	A patient, a patient's representative, a healthcare professional or an authorized supportive 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.
Applicant	User undergoing the processes of enrollment and identity proofing.
Subscriber	A user after successful identification and registration who is has received the authentication means.
Claimant	A subject whose identity is to be verified using one or more authentication protocols.
Attacker	A party who acts with malicious intent to compromise an information system.
Client Platform	The platform from which the user authenticates at the Verifier, e.g., 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.

Table 2: External Entities and Subjects

3.2 Security Problem Definition

The Security Problem Definition describes

c. Assumptions on security relevant properties and behavior of the Target of Evaluation's environment.

d. Organizational security policies, which describe overall security requirements defined by the organization in charge of the overall system including the Target of Evaluation. This may include legal regulations, standards and technical specifications.

e. Threats against the assets, which SHALL be averted by the Target of Evaluation together with its environment.

3.2.1 Assumptions

3.2.1.1 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.

Employees and contractors are assumed to always act with care and according to policies and guidelines of the corresponding part of the Target of Evaluation.

It is assumed, that employees and contractors 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 hand-held device, unless it is securely stored using an approved method.

3.2.1.2 A.AccessManagement

It is assumed, that access management processes and systems are in place to control the allocation of access rights for authorized employees and contractors and to prevent unauthorized access to information systems and to physical premises.

3.2.1.3 A.Physical

It is assumed, that the components of the Target of Evaluation, except for the enrolled authenticator, are operated in a secure area and physically protected against disclosure, manipulations or loss.

3.2.1.4 A.Monitoring

It is assumed, that information processing systems on the service providing part of the Target of Evaluation 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.

3.2.1.5 A.Malware

It is assumed, that information processing systems on the service providing part of the Target of Evaluation 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.

3.2.1.6 A.ClientPlatform

It is assumed, that the client platform used by employees and contractors with access to the Target of Evaluation is protected against malware, has current patch status of all components and is not used with administrator access rights.

3.2.1.7 A.Identification

It is assumed, that all users accessing the Target of Evaluation are identified to the required LOA and IAL, i.e. Subscribers are identified according to the requirements in section 2.5 and employees and contractors accessing the Target of Evaluation Data are identified to the LOA 3 (see fn. 1) and IAL 2 (see fn. 6).

3.2.1.8 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 entity.

In the case of compromise or loss of an authenticator or credential, it is assumed, that the entity informs the service desk of the Identity Provider immediately through appropriate channels to initiate revocation.

3.2.1.9 A.IdentifierGeneration

It is assumed, that the Target of Evaluation implements uses an identifier generation policy which ensures uniqueness of identifiers for Subscribers and impedes cross application identification of Subscriber privacy data.

3.2.1.10 A.SessionManagement

It is assumed, that the Target of Evaluation implements a session management which avoids active sessions, the user is unaware of.

3.2.2 Organizational Security Policies (P)

The Target of Evaluation 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.

3.2.2.1.1 P.Audit

Security relevant events (internal to the Target of Evaluation or due to the communication flows with the Target of Evaluation) 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.

3.2.2.1.2 P.Crypto

State of the art recommended cryptographic functions SHALL be used to perform all cryptographic operations. Cryptographic algorithm known to be unsecure SHALL not be used.

3.2.2.1.3 P.AccessRights

A defined management of access to Target of Evaluation and network resources SHALL be established granting identified and authenticated user 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 Target of Evaluation, 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.

3.2.2.1.4 P.Hardening

A defined policy for hardening the Target of Evaluation SHALL be established and processes SHALL be implemented for the systems to reduce vulnerabilities. To achieve this,

a. Unnecessary software SHALL be removed.
b. Unnecessary services SHALL be disabled or removed.
c. Access to resources SHALL be restricted and controlled.
d. An effective vulnerability and patch management SHALL be established and maintained.

3.2.2.1.5 P.Assertion

Assertions provided by the Verifier or Credential Service Provider to convey identity information on the Claimant/Subscriber SHALL comply with the specification given in this document.

3.2.2.1.6 P.TrustedRelyingPartyEnd-point

An endpoint for secure communication between the Target of Evaluation and the Relying Party SHALL be established. The trusted relying party endpoint SHALL implement the protocols defined in Section 4 of this document.

3.2.3 Threats

This section describes the threats to be averted by the Target of Evaluation independently or in collaboration with its operational environment. These threats apply to the assets protected by the Target of Evaluation and the operational environment. The threats described in chapter 10.3 of (see fn. 1) are covered and extended by the following threats.

3.2.3.1 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 a Credential Service Provider to create a credential based on a fictitious Subscriber/Claimant.

An attacker alters information as it passes from the enrollment 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 Credential Service Provider 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.

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 Verifier updates the latest revocation information.

Attacker:
An attacker alters information during the enrollment 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.

3.2.3.2 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 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), favored by a weak protection mechanism of the authenticator, he can gain authenticated access to the Target of Evaluation.

3.2.3.3 T.WebPlatformAttacks

Asset:
The Target of Evaluation and therefore all assets of the Target of Evaluation.

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.

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 user interface. 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.

Attacker:

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, 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 user interface level, as well as the backend function level since an attacker will ignore the user interface and a forge requests that access unauthorized functionality.

3.2.3.4 T.SpoofingAndMasquerading

Asset:
The Target of Evaluation and therefore all assets of the Target of Evaluation.

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 Verifier with an attackers malicious Verifier or to masquerade a legitimate software publisher responsible for downloading on-line software applications and/or updates by a faked downloading service.

3.2.3.5 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 Verifier, 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 Verifier 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.

3.2.3.6 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.

3.2.3.7 T.ReplayAttack

Asset:
Credentials, authentication exchange data.

Security goal:
The confidentiality of assets.

Adverse action:
An attacker is able to replay previously captured messages (between a legitimate Claimant and a Verifier) to authenticate as that Claimant to the Verifier.

Attacker:
An attacker captures a Claimant’s credential or session IDs from an actual authentication session, then replays it to the Verifier to gain access at a later time.

3.2.3.8 T.Eavesdropping

Asset:
Credentials, authentication exchange data and other TSF or user data.

Security goal:
The confidentiality of communication channels and assets of the Target of Evaluation.

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 Verifier or the Credential Service Provider, so that he can intercept the content of the authentication protocol messages.

Attacker:
An attacker captures the transmission of credentials or Session IDs between Claimant and Verifier or the Credential Service Provider.

3.2.3.9 T.Misconfiguration

Asset:
The Target of Evaluation and therefore all assets of the Target of Evaluation.

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 Target of Evaluation.

Attacker:
An unauthenticated or authenticated attacker is able to exploit a weakness by wrong configuration settings, incomplete deployment, incomplete hardening or not up-to-date software to gain access to confidential information (user or TSF data).

3.2.3.10 T.DoS

Asset:
The Target of Evaluation and therefore all assets of the Target of Evaluation.

Security goal:
Availability of the Target of Evaluation and its assets, since a Denial of Service (DoS) attack aims at making the Target of Evaluation 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 Target of Evaluation or its operating environment by using its own infrastructure or infrastructures taken over.

Attacker:
An (unauthenticated) attacker is able to start a DoS attack onto the external interfaces of the Target of Evaluation (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.

3.2.3.11 T.Man-in-the-middle

Asset:
Credentials, authentication exchange data and other Target of Evaluation security functions or user data.

Security goal:
The confidentiality and integrity of communication channels and assets of the Target of Evaluation to prevent Verifier Impersonation Attacks.

Adverse action:
The Attacker positions himself or herself in between the Claimant and Verifier so that he or she can intercept and alter the content of the authentication protocol messages. The Attacker typically impersonates the Verifier to the Claimant and simultaneously impersonates the Claimant to the Verifier. Conducting an active exchange with both parties simultaneously may allow the Attacker to use authentication messages sent by one legitimate party to successfully authenticate to the other.

Attacker:
An Attacker sets up a fraudulent website impersonating the Verifier. When an unwary Claimant tries to log in using his or her one-time password device, the Attacker's website simultaneously uses the Claimant's one-time password to log in to the real Verifier.

3.2.3.12 T.CrossApplicationIdentification

Asset:
User data in different relying party applications.

Security goal:
Impede building of user profiles of Subscriber by joining the user data using an identifier shared by the relying parties.

Adverse action:
An Attacker is able to cross identify Subscriber data from different relying party systems to build a user profile using the subscriber unique identifier of the Identity Provider.

Attacker:
An Attacker who had access to privacy data of a Subscriber in different Relying Parties uses the subscriber unique identifier of the Identity Provider to build a cross application user profile.

3.2.3.13 T.OrphanedSessions

Asset:
Sessions not closed properly the Subscriber is unaware of.

Security goal:
Ensure that a Subscriber is informed about open sessions when initiating a logout.

Adverse action:
An Attacker is able to adopt an orphaned session of a Subscriber which was active after logout because the Subscriber was not aware of.

Attacker:
An Attacker adopts an orphaned session, when a Subscriber logged out on a relying party application on a device and is not aware of active sessions in other relying party applications on the same or on other devices.

3.3 Security Objectives

This chapter describes the security objectives for the Target of Evaluation and the security objectives for the Target of Evaluation environment.

3.3.1 Security Objectives for the Target of Evaluation

This section describes the security objectives for the Target of Evaluation and addresses the aspects of identified threats to be countered and organizational security policies to be met. The security objectives describe the protection of the primary assets as User Data and the secondary assets as Target of Evaluation Security Functions data (TSF data) against threats.

3.3.1.1 O.Integrity

The Target of Evaluation SHALL protect against either intentional or accidental violation of user and security function data integrity (the property that data has not been altered in an unauthorized manner) and violation of system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).

3.3.1.2 O.Confidentiality

The Target of Evaluation SHALL protect user and security function data against intentional or accidental attempts to perform unauthorized access. The Target of Evaluation SHALL protect confidentiality of user and security function data in storage, during processing and while in transit.

3.3.1.3 O.Availability

The Target of Evaluation SHALL ensure the availability of services and the security functions to authorized users (e.g. the Verifier or the Credential Service Provider becoming unavailable to Subscribers as a consequence of a DoS attack or insufficient scalability).

3.3.1.4 O.Accountability

The Target of Evaluation SHALL trace all actions of an entity uniquely to that entity. The Target of Evaluation 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.

3.3.1.5 O.Authentication

Security measures shall be applied to protect an access point or a communication system against acceptance of fraudulent access or transmission. A cryptographic protocol to guarantee the authenticity and the validity designed for the transfer of authentication data between the authenticator and the verifier shall ensure that no authentication data can be read out or used to gain access or to inject the communication channel by attackers or third parties

3.3.1.6 O.SecureCommunication

The Target of Evaluation 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.

3.3.1.7 O.CryptographicFunctions

The Target of Evaluation SHALL provide means to encrypt and decrypt user data and Target of Evaluation security function data to maintain confidentiality, integrity and accountability and to allow for detection of modification of user data transmitted within or outside of the Target of Evaluation.

3.3.1.8 O.AccessControl

The Target of Evaluation SHALL enforce access control on all objects of the Target of Evaluation (e.g. assets) as well as the Target of Evaluation security function to prevent unauthorized use.

3.3.1.9 O.IdentifierGeneration

The Target of Evaluation SHALL use Subscriber identifier which are unique for the combination of the Subscriber, the Relying Party and the Identity Provider to impede cross application identification. The Subscribers identifier SHALL be kept confidential and never presented to the Claimant, the User Agent or third party systems.

3.3.1.10 O.SessionManagement

If the Target of Evaluation supports per session logout, the Target of Evaluation SHALL fulfill the following requirement: When a Subscriber logs out from a relying party, the Verifier SHALL present the Subscriber a screen of all active sessions of the Subscriber and enable the Subscriber to terminate active sessions from the user interface.

3.3.2 Security Objectives for the operational environment

This section describes security objectives the Target of Evaluation SHALL address in the operational environment to solve problems with regard to the threats and organizational security policies.

3.3.2.1 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 SHALL be 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:

a. ISO/IEC 27001: A.7 Human resource security[7].

3.3.2.2 OE.AccessManagementSystem

Secure Operation of the Target of Evaluation 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:

a. ISO/IEC 27001: A.9 Access Control (reference see fn. 7).

3.3.2.3 OE.SecureAreasAndEquipment

Critical or sensitive information processing facilities of the Target of Evaluation 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:

a. ISO/IEC 27001: A.11 Physical and environmental security (reference see fn. 7).

3.3.2.4 OE.ConfigurationAndChangeManagement

In order to ensure the integrity of information processing systems of the Target of Evaluation, there SHALL be established strict controls over the implementation of changes. Formal change control procedures SHALL be enforced. The Identity Provider, the Registration and Local Registration Authorities SHALL 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 (reference see fn. 7):

a. ISO/IEC 27001: A.12.1.2 Change management.

b. ISO/IEC 27001: A.12.5 Control of operational software.

3.3.2.5 OE.MalwareAndVulnerabilityManagement

The Verifier, Credential Service Provider and the information processing systems of the Registration and Local Registration Authorities 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.

[7] ISO/IEC 27001:2013, Cor. 1:2014 and 2:2015: Information technology -- Security techniques -- Information security management systems – Requirements.

When a potential technical vulnerability has been identified, associated risks SHALL be identified and the following actions SHALL be taken:

a. Patching the vulnerable systems or turning off services or capabilities related to the vulnerability.
b. Adapting or adding access controls, e.g. firewalls.
c. Increased monitoring to detect actual attacks.
d. Raising awareness of the vulnerability.

The following controls SHALL be applied and fulfilled (reference see fn. 7):

e. ISO/IEC 27001: A.12.2 Protection from malware.
f. ISO/IEC 27001: A.12.6 Technical vulnerability management.

3.3.2.6 OE.LoggingAndMonitoring

The information processing systems of the Verifier, Credential Service Provider, the Registration and Local Registration Authorities 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 (reference see fn. 7):

a. ISO/IEC 27001: A.12.4 Logging and monitoring.

3.3.2.7 OE.NetworkSecurity

A policy concerning the use of networks and network services of the information processing systems of the Verifier, Credential Service Provider, the Registration and Local Registration Authorities SHALL be defined and 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 Verifier and the Credential Service Provider 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 (reference see fn .7):

a. ISO/IEC 27001: A.13.1 Network security management.

3.3.2.8 OE.OperationsSecurity

The information processing systems of the Verifier, Credential Service Provider, the Registration and Local Registration Authorities SHALL ensure correct and secure operations of information processing systems.

The following controls SHALL be applied and fulfilled (all from reference fn. 7):

a. ISO/IEC 27001: A.12.3 Backup.
b. ISO/IEC 27001: A.14.2.1 Secure development policy.
c. ISO/IEC 27001: A.14.2.5 Secure system engineering principles.
d. ISO/IEC 27001: A.15 Supplier relationships.
e. ISO/IEC 27001: A.16 Information security incident management.
f. ISO/IEC 27001: A.18.1.3 Protection of records.
g. ISO/IEC 27001: A.18.1.4 Privacy and protection of personally identifiable information.
h. ISO/IEC 27001: A.18.2.2 Compliance with security policies and standards.
i. ISO/IEC 27001: A.18.2.3 Technical compliance review.

3.3.2.9 OE.DataLifecycleMangement

The information processing systems of the Verifier, Credential Service Provider, the Registration and Local Registration Authorities SHALL manage the identity data lifecycle. The following requirements and controls SHALL be fulfilled:

a. The Target of Evaluation SHALL provide policies for managing the identity information lifecycle.

b. The system of storage and handling SHALL ensure identification of records and a retention period of 11 years after closure of the subscribers account. This system SHALL permit appropriate destruction of records after the retention period if there are no other legal regulations, which prevent the destruction of the records.

c. Policies to specify the conditions and procedures to archive identity information SHALL be established by the Registration and Local Registration Authorities.

d. The Target of Evaluation SHALL provide policies to specify the conditions and procedures to initiate deletion of identity information.

The following controls SHALL be applied and fulfilled[8]:

e. ISO/IEC 24760-2: 6.3.1 Policies for identity information lifecycle.

f. ISO/IEC 24760-2: 6.3.7 Termination and Deletion of identity information.

3.3.2.10 OE.CredentialManagement

The information processing systems of the Verifier, Credential Service Provider, the Registration and Local Registration Authorities SHALL fulfil the following requirements on credential management:

a. The Credential Service Provider, the Registration and Local Registration Authorities SHALL establish and maintain formalized and documented processes for credential creation.

b. Prior to finalizing the binding of a credential to an entity, the Registration and the Local Registration Authorities SHALL have adequate assurance that the credential is bound and remains bound to the correct entity and is protected against tampering. The Registration and Local Registration Authorities SHALL create a record containing the date and time the authenticator was bound to the account. This record SHOULD include information about the source of the binding (e.g., IP-Address, device identifier) of any device associated with the enrollment. If available, the record SHOULD also contain information about the source of unsuccessful authentications attempted with the authenticator.

c. If a credential, or the means used by the Credential Service Provider to produce credentials, is held on a hardware device, the hardware device SHALL be kept physically secure and the inventory tracked.

d. The Registration and Local Registration Authorities SHALL establish and maintain formalized and documented processes for credential issuance.

e. The Registration and Local Registration Authorities SHALL implement a procedure to ensure that a credential, or means to generate a credential, is activated only if it is under the control of the intended Subscriber. This procedure SHALL prove that the entity is bound to activation of a credential (e.g. challenge-response protocol).

f. Protection policy for stored credentials SHALL be described in the documentation associated with the use of those credentials that is made available to Subscribers.

g. A record of the registration, history, and status of each credential (including revocation) SHALL be maintained by the Credential Service Provider.

The following controls SHALL be applied and fulfilled (all from reference fn. 1):

h. ISO/IEC 29115: 10.2.2.1: #1.

i. ISO/IEC 29115: 10.2.2.1: #2.

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

j. ISO/IEC 29115: 10.2.2.1: #5.
k. ISO/IEC 29115: 10.2.2.1: #6.
l. ISO/IEC 29115: 10.2.2.1: #7.
m. ISO/IEC 29115: 10.2.2.1: #10.
n. ISO/IEC 29115: 10.2.2.1: #12.
o. ISO/IEC 29115: 10.2.2.1: #13.
p. ISO/IEC 29115: 10.2.2.1: #14.
q. ISO/IEC 29115: 10.2.2.1: #20.
r. ISO/IEC 29115: 10.2.2.1: #21.

3.3.2.11 OE.UserSecurityAwareness

The information processing systems of the Verifier, Credential Service Provider, the Registration and Local Registration Authorities SHALL fulfil the following requirements to ensure security awareness of operators and administrative users:

a. Operators and administrative users SHALL receive awareness education and training and regular updates in organizational policies and procedure.
b. Operators and administrative users SHALL agree to protect his authenticator and exercise care to prevent any unauthorized use of its authenticator.
c. Operators and administrative users SHALL keep their computing environment 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.

The following controls SHALL be applied and fulfilled (all references see fn. 7):

d. ISO/IEC 27001: A.7.2.1 Management responsibilities.
e. ISO/IEC 27001: A.7.2.2 Information security awareness, education and training.
f. ISO/IEC 27001: A.7.2.3 Disciplinary process.
g. ISO/IEC 27001: A.7.3.1 Termination or change of employment responsibilities.

3.3.3 Security Objective rationale

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

3.3.3.1 Countering the threats

3.3.3.1.1 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 Target of Evaluation.

3.3.3.1.2 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 Target of Evaluation.

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

3.3.3.1.3 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 Target of Evaluation s 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.

3.3.3.1.4 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 Target of Evaluation 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 re-quires any message to be digitally signed and O.SecureCommunication that secure communication is supported by the Target of Evaluation. The objective OE.LoggingAndMonitoring further requires logs and fault logging to ensure information that system problems are identified.

3.3.3.1.5 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 Verifier 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 Target of Evaluation environment OE.NetworkSecurity.

3.3.3.1.6 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 against 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 Target of Evaluation environment OE.LoggingAndMonitoring.

3.3.3.1.7 T.ReplayAttack

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

The protection against this threat is achieved by the security objectives O.Accountability, O.SecureCommunication, specifically providing nonce or challenges to prove the freshness of the transaction and supportively by the objective for the Target of Evaluation environment OE.LoggingAndMonitoring.

3.3.3.1.8 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 against this threat is achieved by the security objectives O.Confidentiality, O.SecureCommunication, specifically encrypting all communication appropriately and supportively the objective for the Target of Evaluation environment OE.NetworkSecurity.

3.3.3.1.9 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 against this threat is achieved by the security objectives for the Target of Evaluation environment OE.HR_Security and OE.ConfigurationAndChangeManagement.

3.3.3.1.10 T.DoS

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

The protection against this threat is achieved by the security objectives O.Availability and the objectives for the Target of Evaluation environment OE.ConfigurationAndChangeManagement, OE.MalwareAndVulnerabilityManagement and OE.NetworkSecurity.

3.3.3.1.11 T.Man-in-the-Middle

The threat T.Man-in-the-Middle addresses verifier impersonation attacks focusing on TOE Security Function in order to pretend a Subscriber/Claimant and fake the access control sessions to get unauthorized access.

The protection against this threat is achieved by the security objectives O.Integrity**,** O.Confidentionality, O.Authentication**,** O.SecureCommunication and the objectives for the TOE environment OE.NetworkSecurity and OE.CredentialManagement.

3.3.3.1.12 T.CrossApplicationIdentification

The threat T.CrossApplicationIdentification adresses attacks where an attacker is able to cross identify Subscriber data from different relying party systems to build a user profile using the subscriber unique identifier of the Identity Provider.

The protection against this threat is achieved by using subscriber identifier which are unique combination of the Subscriber, the Relying Party and the Identity Provider defined in the objectove O.IdentifierGeneration.

3.3.3.1.13 T.OrphanedSessions

The threat T.OrphanedSessions adresses attacks to adopt orphaned sessions of a Verifier which supports session based logout.

The protection against this threat is achieved by O.SessionManagement.

3.4 Security Requirements

3.4.1 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 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 Protection Profile 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 Protection Profile 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*.

The iteration operation is used repeat the same component, but applying assignment, selections or refinements in a different way.

3.4.2 Security Functional Requirements for the Target of Evaluation

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

3.4.2.1 Security audit automatic response (FAU_ARP)

FAU_ARP.1 Security alarms	
FAU_ARP.1.1	The TSF SHALL take [<u>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*</u>] upon detection of a potential security violation.
Hierarchical to:	No other components.
Dependencies:	**FAU_SAA.1 Potential violation analysis**
Application note:	The security alarms have to be integrated in the monitoring processes of the computing environment of the Target of Evaluation.

3.4.2.2 Audit Data Generation (FAU_GEN)

<table>
<tr><th colspan="2">FAU_GEN.1 Audit data generation</th></tr>
<tr><td>FAU_GEN.1.1</td><td>The TSF SHALL generate audit records for the following events related to the authentication of Subscriber:
<table>
<tr><th>Event</th><th>Additional Details</th></tr>
<tr><td>Authentication successful</td><td>– Subscriber ID
– IP address
– Final status
– Referrer header field
– Time of event</td></tr>
<tr><td>Authentication unsuccessful</td><td>– Claimant ID
– IP address
– Final status
– Error message
– Referrer header field
– Time of event</td></tr>
<tr><td>Logout successful</td><td>– Subscriber ID
– IP address
– Final status
– Time of event</td></tr>
<tr><td>Logout unsuccessful</td><td>– Subscriber ID
– IP address
– Final status
– Error message
– Time of event</td></tr>
</table></td></tr>
<tr><td>FAU_GEN.1.2</td><td>The TSF SHALL generate audit records for the following events related to the activities of privileged accounts, e.g. supervisor, root, administrator:
<table>
<tr><th>Event</th><th>Additional Details</th></tr>
<tr><td>Creation of a Subscriber</td><td>– Subject ID
– Subject name
– Subject role
– Subscriber ID
– Final status
– Time of the event</td></tr>
<tr><td>Deletion of a Subscriber</td><td>– Subject ID
– Subject name
– Subject role
– Subscriber ID
– Final status
– Time of the event</td></tr>
<tr><td>Locking and Unlocking of Subscriber</td><td>– Subject ID
– Subject name
– Subject role
– Subscriber ID
– Final status
– Time of the event</td></tr>
<tr><td>Successful and rejected access attempts to data and resources</td><td>– Subject ID
– Subject name
– Subject role
– Resources (e.g., files) accessed
– Time of the event</td></tr>
</table></td></tr>
</table>

	<table><tr><td>Changes to system configuration</td><td>– Subject ID – Subject name – Subject role – Configuration change – Time of the event</td></tr><tr><td>Privileged actions (e.g. password change)</td><td>– Subject ID – Subject name – Subject role – Action – Time of the event</td></tr></table>
FAU_GEN.1.3	The TSF SHALL generate audit records for the following system events: <table><tr><th>Event</th><th>Additional Details</th></tr><tr><td>Login successful</td><td>– Subject ID – Subject name – Subject role – Final status – Time of the event</td></tr><tr><td>Logout successful</td><td>– Subject ID – Subject name – Subject role – Final status – Time of the event</td></tr><tr><td>Logon failure</td><td>– Subject ID – Subject name – Subject role – Final Status – Time of the event</td></tr><tr><td>Use of system utilities and applications</td><td>– Subject ID – Subject name – Subject role – Name of utility or application – Time of the event</td></tr><tr><td>I/O device/connector attachment/detachment</td><td>– Device ID – Device Type – Time of the event</td></tr><tr><td>Alarms raised by the access control system</td><td>– Entity – Alarm Type – Time of the event</td></tr><tr><td>Network management alarms</td><td>– Entity – Alarm Type – Time of the event</td></tr><tr><td>Activation and de-activation of protection systems</td><td>– Subject ID – Subject name – Subject role – Final Status – Name of protection system – Time of the event</td></tr><tr><td>System start and stop</td><td>– Subject ID – Subject name – Subject role – Final Status – System Name</td></tr></table>

	– Time of the event
Hierarchical to:	No other components.
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 Target of Evaluation.

3.4.2.3 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 known to indicate a potential security violation. b) none.
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 Target of Evaluation

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

3.4.2.4 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 with the capability to read incident and activity log 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 Target of Evaluation
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:	

3.4.2.5 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 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 to the Verifier and the Credential Service Provide, including the and Local Registration Authorities and SHALL be integrated into the operation security concept of the computing environment of the Target of Evaluation.

3.4.2.6 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 and specified cryptographic key sizes which are derived from the technical guideline BSI TR-02102-1 - “Cryptographic Mechanisms: Recommendations and Key Lengths” of the German Federal Office for Information Security. Recommended algorithms and cryptographic key sizes are documented in page 15, table 1.2, Version 2021-01) of the referenced document. Cryptographic key generation for used cryptographic algorithms should meet the requirements of NIST Special Publication 800-133 “Recommendation for Cryptographic Key Generation” (Revision 2).
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 in accordance with a specified cryptographic key access method import through a secure channel that meets the following: GlobalPlatform Card Specification v.2.3 [11], TLSv1.2[9] or higher, other equivalent secure means with defined descriptions.
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:	
FCS_CKM.4 Cryptographic key destruction	

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

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 that meets the following: none.
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).

3.4.2.7 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 in accordance with a secure cryptographic algorithm defined in the technical guideline BSI TR-02102-1 - "Cryptographic Mechanisms: Recommendations and Key Lengths" (Version 2021-01) of the German Federal Office for Information Security. Secure parameters for symmetric key cryptographic operations (block cipher algorithms, operational modes and paddings schemes) are documented in page 21-24, table 2.1, 2.2 and 2.3 within the referenced document.
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 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 in accordance with a secure cryptographic algorithm according to the technical guideline BSI TR-02102-1 - "Cryptographic Mechanisms: Recommendations and Key Lengths" (Version 2021-01) of the German Federal Office for Information Security. Secure parameters for asymmetric key cryptographic operations are documented in page 27, table 3.1 (algorithms and sizes) and page 38 table 3.3 (padding scheme for RSA) within the referenced document.
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 in accordance with a secure cryptographic hash algorithm according to the technical guideline BSI TR-02102-1 - "Cryptographic Mechanisms: Recommendations and Key Lengths" (Version 2021-01) of the German Federal Office for Information Security. Secure cryptographic hashing algorithms and key sizes are documented on page 39 table 4.1 of the referenced document.
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:	

3.4.2.8 Access control policy (FDP_ACC)

FDP_ACC.1 Subset access control	
FDP_ACC.1.1	The TSF SHALL enforce the access control SFP on user, trusted user, temporary privileged users, user data and operations among subjects and objects covered by the SFP.
Hierarchical to:	No other components.
Dependencies:	**FDP_ACF.1 Security attribute based access control**
Application note:	None

3.4.2.9 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 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.
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.
FDP_ACF.1.3	The TSF SHALL explicitly authorize access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4	The TSF SHALL explicitly deny access of subjects to objects based on the following additional rules: none.
Hierarchical to:	No other components.
Dependencies:	**FDP_ACC.1 Subset access control** **FMT_MSA.3 Static attribute initialization**
Application note:	These requirements apply to the Verifier and the Credential Service Provider, including the Registration and Local Registration Authorities and SHALL be integrated into the access management system of the computing environment of the Target of Evaluation.

3.4.2.10 Import from outside of the Target of Evaluation (FDP_ITC)

FDP_ITC.2 Import of user data with security attributes	
FDP_ITC.2.1	The TSF SHALL enforce the access control SFP when importing user data, controlled under the SFP, from outside of the Target of Evaluation.
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 Target of Evaluation: none.
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

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

3.4.2.12 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 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.
Dependencies:	**FIA_UID.1 Timing of identification**
Application note:	
FIA_UAU.3 Unforgeable authentication	
FIA_UAU.3.1	The TSF SHALL detect and prevent use of authentication data that has been forged by any user of the TSF.
FIA_UAU.3.2	The TSF SHALL detect and prevent 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:

	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) 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 Target of Evaluation 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.
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	
FIA_UAU.6.1	The TSF SHALL re-authenticate the user under the conditions: using their primary authentication mechanism or an appropriate subset thereof.
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 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.

3.4.2.13 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 (restricted to the functions and resources accessible to the Subscriber/Claimant according to the access control policy assigned for that purpose) 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:	

3.4.2.14 User-subject binding (FIA_USB)

FIA_USB.1 ID policy	
FIA_USB.1.1	The TSF SHALL generate Subscriber identifier which are unique for the combination of the Subscriber, the Relying Party and the Identity Provider to impede cross application identification.
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	

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

3.4.2.16 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 to restrict the ability to query, delete the security attributes Reference of the user credential, Claimant ID, Identification Data to Trusted User.
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	
FMT_MSA.3.1	The TSF SHALL enforce the access control SFP to provide restrictive default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF SHALL allow the Security Information Officers 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

3.4.2.17 Revocation (FMT_REV)

FMT_REV.1 Revocation	
FMT_REV.1.1	The TSF SHALL restrict the ability to revoke security attributes associated with the users under the control of the TSF to the authorized Subscriber/Claimant.
FMT_REV.1.2	The TSF SHALL enforce rules The TSF SHALL revoke immediately the authentication associated with security incidents The authorized Claimant SHALL revoke the authentication capabilities and means provided by the Subscriber/Claimant and the registration authority according to the applicable policies.
Hierarchical to:	No other components.
Dependencies:	**FMT_SMR.1 Security roles**
Application note:	The Verifier SHALL provide a revocation service.

3.4.2.18 Specification of Management Functions (FMT_SMF)

FMT_SMF.1 Specification of Management Functions	
FMT_SMF.1.1	The TSF SHALL be capable of performing the following security management functions: – Management of security attributes objects and credentials – Management of claimant security attributes – Management of authentication data – Management of audit trail – Management of audited events – Management of Target of Evaluation access banner – Management of role definitions, including role hierarchies and constraints – Management of access control and its policy – Management of Target of Evaluation configuration data – Management of cryptographic network protocols – Management of cryptographic keys – Management of digital certificates – Management of identification and authentication policy – Management of identity – Management of session services – Management of authenticator – Management of reference authentication data
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	None

3.4.2.19 Security management roles (FMT_SMR)

FMT_SMR.1 Security roles	
FMT_SMR.1.1	The TSF SHALL maintain the roles: - Administrator, - Operator, - Service, - Claimant, - Subscriber, - Applicant, - and further authorized roles (e.g. supervisors).
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

3.4.2.20 Replay detection (FPT_RPL)

FPT_RPL.1 Replay detection	
FPT_RPL.1.1	The TSF SHALL detect replay for the following entities: TSF data and security attributes.
FPT_RPL.1.2	The TSF SHALL perform reject data and audit event when replay is detected.
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	

3.4.2.21 Time stamps (FPT_STM)

FPT_STM.1 Reliable time stamps	
FPT_STM.1.1	The TSF SHALL be able to provide reliable time stamps.

Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	These requirements apply to the Verifier and Credential Service Provider, including the Registration and Local Registration Authorities and SHALL be integrated into the logging and monitoring concept of the computing environment of the Target of Evaluation.

3.4.2.22 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 when shared between the TSF and another trusted IT product.
FPT_TDC.1.2	The TSF SHALL use the message definitions of section 4.1 or section 4.2 when interpreting the TSF data from another trusted IT product.
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	None

3.4.2.23 Limitation on scope of selectable attributes (FTA_LSA)

FTA_LSA.1 Limitation on scope of selectable attributes	
FTA_LSA.1.1	The TSF SHALL restrict the scope of the session security attributes cookies, session-IDs, based on user identity, originating location, time of access.
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	

3.4.2.24 Confidentiality of exported TSF data (FTP_ITC)

FTP_ITC.1 Inter-TSF confidentiality transmission	
FTP_ITC.1.1	The TSF SHALL provide communication channels to trusted IT products that are logically distinct from other communication channels (e.g., out-of-band) 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 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.
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	This is to protect the transmission between the components of the Verifier, Credential Service Provider, Registration and Local Registration Authorities and other trusted IT products required for TOE operation. The TSF SHALL only use TLS 1.2 or higher, or IPsec with IKEv2 (RFC 4301 [9], RFC 7296 [10]) for communication channel to other trusted IT Products.

3.4.2.25 Session Management (FTA_SSL)

FTA_SSL.1 Session Overview	
FTA_SSL.1.1	If the Identity Provider supports per session logout and a Subscriber logs out from a relying party, the Verifier SHALL present a user interface displaying all active sessions of the Subscriber from which the Subscriber is able to terminate active sessions.
Hierarchical to:	No other components.
Dependencies:	No dependencies.

Application note:	

3.4.3 Security Requirements Rationale

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.

The security objective **O.IdentifierGeneration** is enforced by the following security functional requirements:

- FIA_USB.1: User-subject binding.

The security objective **O.SessionManagement** is enforced by the following security functional requirements:

- FTA_SSL.1: Session Management.

3.5 Security Assurance Requirements

3.5.1 Security architecture description

The Identity Provider shall provide a security architecture description of the Target of Evaluation and its security functions. The security architecture description SHALL:

a. Be at a level of detail commensurate with the requirements of this protection profile.
b. Describe how the Target of Evaluation initialisation process is secure.
c. Demonstrate that the Target of Evaluation protects itself from tampering.
d. Demonstrate that the Target of Evaluation prevents bypass of the security functions.

3.5.2 Security enforcing functional specification

The Identity Provider shall provide a functional specification of the Target of Evaluation security functions. The functional specification SHALL:

a. Describe the purpose and method of use of the security functions interfaces.
b. Identify and describe the parameters associated with each security function interfaces.
c. Describe the enforcing actions associated with the security function interfaces.
d. Describe the error messages resulting from processing of the security function interfaces.
e. Link all security function interfaces to the relevant security functional requirements.

3.5.3 Basic Design

The Identity Provider shall provide a design description of the Target of Evaluation. The basic design description SHALL:

a. Describe the structure of the Target of Evaluation in terms of subsystems.
b. Identify all subsystems of the Target of Evaluation security functions.
c. Provide a behaviour summary of each Target of Evaluation security function.
d. Provide a description of the interactions among the Target of Evaluation security functions.

3.5.4 Guidance Documents

The Identity Provider shall provide operational user guidance of the Target of Evaluation. The operational user guidance SHALL:

a. Describe for each user role the user-accessible functions and privileges that should be controlled in a secure processing environment.
b. Describe for each user role how to use the available interfaces provided by the Target of Evaluation in a secure manner.
c. Present for each user role the types of security-relevant events relative to the user-accessible functions that need to be performed.
d. Identify the modes of operation of the Target of Evaluation including operation following failure or operational errors, their consequences and implications for maintaining the secure operation.
e. Describe the security measures to be followed in order to fulfil the security objectives for the operational environment.

3.5.5 Testing of Security Functional Requirements

The Identity Provider SHALL perform all Security Functional Requirement Testing in accordance with the following requirements:

a. The test protocol SHALL have defined expected results vs actual results.
b. The documentation of the results from testing SHALL include evidences of the results.
c. The actual test results SHALL be consistent with expected results prior to productive release of changes.
d. The results of testing SHALL be reviewed by an approver separate from the developer and tester prior to productive release of changes.
e. The tests SHALL be mapped to the corresponding interfaces and security functional requirements.

3.5.6 Preparative procedures

The Identity Provider shall provide a description of the preparative procedures for ensuring that the Authenticator has been received and installed in a secure manner as intended by the Identity Provider. The description of the preparative procedures SHALL:

a. Describe all steps necessary for secure acceptance of the Authenticator in accordance with the developer's delivery procedures.
b. Describe all steps necessary for secure installation of the Authenticator.
c. Describe all steps for the secure preparation of the operational environment of the Authenticator.

3.5.7 Vulnerability analysis

The Identity Provider shall provide the Target of Evaluation for testing of the security functions (i.e., penetration tests) by the certification criteria evaluator.

3.5.8 Internal Audit

The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:

The organization shall plan, establish, implement and maintain an audit program, including the frequency, methods, responsibilities, planning requirements and reporting.

The internal audit program shall take into consideration the importance of the processes concerned and the results of previous audits, define the audit criteria and scope for each audit, select auditors and conduct audits that ensure objectivity and the impartiality of the audit process, ensure that the results of the audits are reported to relevant management and retain documented information as evidence of the internal audit program and the audit results.

3.5.9 Management Review

The responsible leadership management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The management review shall include consideration of:

a. the status of actions from previous management reviews;
b. changes in external and internal issues that are relevant to the information security management system;
c. feedback on the information security performance, including the improvement status of non-conformities and corrective actions;
d. monitoring and measurement results;
e. fulfilment of information security objectives;
f. results of risk assessment and status of risk treatment plan;
g. the outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

The organization shall retain documented information as evidence of the results of management reviews.

3.5.10 Plan Do Check Act - Improvement Cycle

When a nonconformity occurs, the organization shall react to the non-conformity, and as applicable:

a. take action to control and correct it;
b. deal with the consequences;
c. valuate the need for action to eliminate the causes of nonconformity, in order that it does not recur by:
    I. Reviewing the non-conformity;
    II. determining the causes of the nonconformity;
    III. determining if similar nonconformities exist, or could potentially occur;
    IV. implement any action needed;
    V. review the effectiveness of any corrective action taken;
    VI. make changes to the information security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered. The organization shall retain documented information as evidence of:

d. the nature of the nonconformities and any subsequent actions taken
e. the results of any corrective action.

4 Protocol Requirements

4.1 SAML 2.0 Binding

Verifier SHALL provide trusted endpoints for Relying Parties implementing the SAML 2.0 Artifact Binding with Artifact Resolution Protocol via SOAP back-channel fulfilling the requirements defined in this section.

4.1.1 Sequences

4.1.1.1.1 Authentication

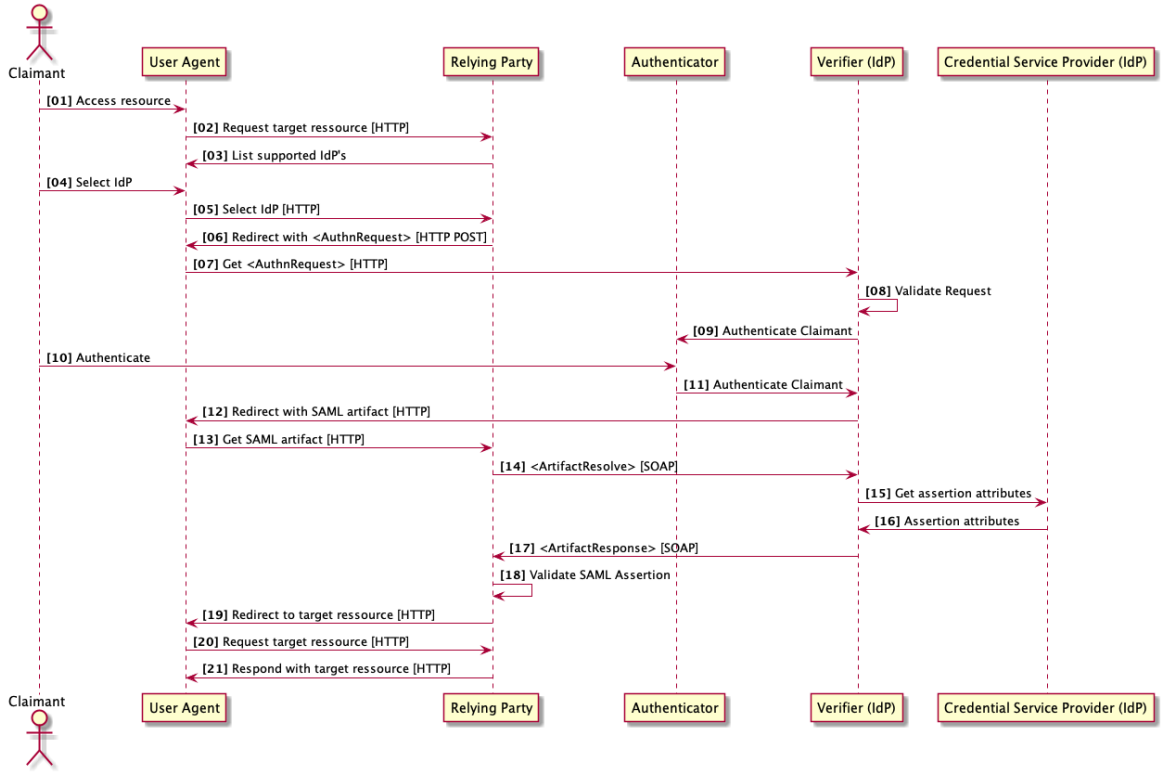

Figure 2: Authentication-Sequence with SAML 2 Artifact Binding

SEQ	Description
01,02	The Claimant's user agent attempts to access a resource on the relying party.
03	The Relying Party presents the list of supported Verifiers to the Claimant.
04,05	The Claimant selects a Verifier.
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.
08	The Verifier determines whether the Claimant has an existing logon security context that meets the default or requested authentication policy requirements. If not, the Verifier interacts with the browser to challenge the Claimant to provide valid credentials.
09…11	The Verifier communicates with the Authenticator(s) to authenticate the Claimant. The Claimant provides valid credentials and the Verifier creates a local logon security context for the Claimant.
12,13	The Verifier 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.
14	The Relying Party 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 Verifier. This exchange is performed using a synchronous SOAP message exchange over the back-channel.
15,16	The Verifier extracts the MessageHandle from the artifact and requests the assertion or assertion attributes message associated with the artifact.
17	The Verifier returns the assertion with a SAML <ArtifactResponse> message as SOAP message via the back-channel to the Relying Party.
18…21	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.

Table 3: Authentication-Sequence with SAML 2 Artifact Binding

Relying Parties MAY renew SAML Identity Assertions for the duration of the Verifier's idle time of 2 hours after the assertion lifetime has expired without requiring a new authentication of the Claimant. To fulfill this requirement, the Verifier SHALL publish a web service endpoint, which implements a Security Token Service as defined in the WS-Security Standard[10].

4.1.1.2 Renew

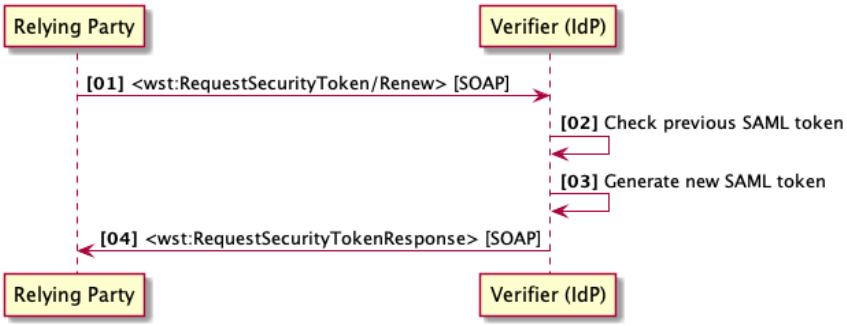

Figure 3: Renewal of a SAML-Assertion

SEQ	Description
01	The Relying Party uses the Identity Assertion of the Claimant in a <RequestSecurityToken> request as defined to the WS-Security Standard and sends it to the Verifier as SOAP version 1.1 request via the back-channel.

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

SEQ	Description
02	The Verifier validates the signature of the request and the signature of the assertion conveyed in the request.
03	The Verifier generates a new SAML Identity Assertion with a new expiration semantics according to chapter 6.3.
04	The Verifier embeds the generated SAML Identity Assertion in the <RequestSecurityToken-Response> according to the WS-Security Standard. Subsequently the Verifier sends this token as SOAP version 1.1 response message via the back-channel.

Table 4: Renewal of a SAML-Response-Assertion with new expiration semantics

4.1.1.3 Logout

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. Verifier, Relying Parties and Other Session Participants shall fulfill the following requirements:

a. Relying Parties SHALL cryptographically sign the <LogoutRequest> and <LogoutResponse> messages and the Verifier SHALL validate the signature with the public key of a pre-registered X.509 certificate.

b. The X.509 certificate used by Relying Parties for signatures of the <LogoutRequest> message SHALL be issued by a managed Certificate Authority (CA) that is operated according to documented processes detailed in a Certificate Policy (CP) and Certificate Practice Statement (CPS). The CA's processes should meet the requirements of class 1 certificates defined within the eCH-0048 PKI Certificate Classes standard (Version 2.0).

c. The X.509 certificate used by Relying Parties for TLS authentication of the endpoit to receive of <LogoutRequest> messages from the Verifier SHALL be issued by a managed Certificate Authority (CA) that is operated according to documented processes detailed in a Certificate Policy (CP) and Certificate Practice Statement (CPS). The CA's processes should meet the requirements of class 1 certificates defined within the eCH-0048 PKI Certificate Classes standard (Version 2.0).

d. During logout propagation Verifiers SHALL cryptographically sign the <LogoutRequest> messages and the Other Session Participant SHALL validate the signature.

e. The X.509 certificate used for signatures by the Verifier SHALL be issued by a trusted certificate service provider according to ZertES; SR 943.03 and listed by the Swiss Accreditation Service (SAS).

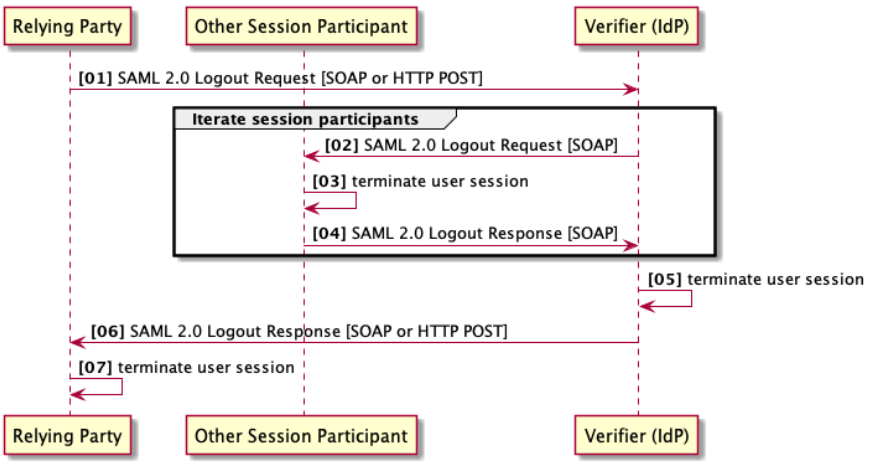

Figure 4: SAML 2.0 Logout Sequence

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 Verifier using the SAML 2 http POST or SOAP Binding.

SEQ	Description
02	The Verifier determines the other session participants and sends a <LogoutRequest> message using the SOAP Binding.
03,04	The other session participants terminate their user session and send a <LogoutResponse> message to the Verifier using the SOAP Binding.
05,06	The Verifier terminates the session and responds to the initial <LogoutRequest> with a <LogoutResponse> using the SAML 2 http POST or SOAP Binding.
07	The initiating Relying Party terminates the user session.

Table 5: SSO Logout Sequence

4.1.2 Protocol Requirements

4.1.2.1 Front-channel Communication

The User Agent and the Verifier SHALL communicate through an authenticated protected channel using TLS 1.2 or higher. The User Agent can either authenticate itself with TLS Client authentication or using digital signature mechanisms on a message level.

The Verifier SHALL identify and authenticate itself with X.509 certificates which are issued by a trusted certificate service provider according to ZertES; SR 943.03 and listed by the Swiss Accreditation Service (SAS).

Relying Parties and Authenticators which communicate with the Verifier through an intermediary user agent SHALL use digital signatures for message level authentication. The X.509 certificates used for signatures SHALL be issued by a managed Certificate Authority (CA) that is operated according to documented processes detailed in a Certificate Policy (CP) and Certificate Practice Statement (CPS). The CA's processes SHALL meet the requirements of class 1 certificates defined within the eCH-0048 PKI Certificate Classes standard (Version 2.0).

4.1.2.2 Back-channel Communication

The Verifier SHALL communicate with Relying Parties through an authenticated and protected back-channel (e.g., IPsec, TLS 1.2 or higher) for artefact resolution, token renew and logout. The Verifier SHALL identify and authenticate itself with TLS authentication or, when sending logout requests with message level authentication using X.509 certificates issued by a class 2 TLS certificate issued by a trusted certificate service provider according to ZertES; SR 943.03 and listed by the Swiss Accreditation Service (SAS).

The Verifier SHALL NOT use redirects through an intermediary user agent (e.g., Web Browser) to communicate with Relying Parties for artefact resolution, token renew and logout.

Relying Parties SHALL use message level authentication (e.g., digital signature) to identify and authenticate. Relying Parties SHALL use X.509 certificates issued by a managed Certificate Authority (CA) that is operated according to documented processes detailed in a Certificate Policy (CP) and Certificate Practice Statement (CPS) to identify and authenticate themselves for artefact resolution, token renew and logout. The CA's processes SHALL meet the requirements of class 1 certificates defined within the eCH-0048 PKI Certificate Classes standard (Version 2.0).

4.1.3 Messages

4.1.3.1 Authentication Request

The <AuthnRequest> message SHALL be used by the Relying Party to initiate the authentication sequence.

The <AuthnRequest> message SHALL be cryptographically signed by the Relying Party and the Verifier SHALL validate the signature. The signature SHALL be asymmetric using X.509 certificates issued by a managed Certificate Authority (CA) that is operated according to documented processes detailed in a Certificate Policy (CP) and Certificate Practice Statement (CPS). The CA's processes should meet the requirements of class 1 of the eCH-0048 PKI Certificate Classes standard.

The signature SHALL either be validated with the public key of a pre-registered X.509 certificate, or the embedded certificate. If the public key of the embedded certificate is used, the Verifier SHALL verify, that the certificate matches the pre-registered one.

4.1.3.2 Authentication Response

The Authentication Response message SHALL be used by the Verifier as response to the <AuthnRequest> message to convey the artifact after authenticating the Claimant/Subscriber.

The Artifact conveyed with Authentication Response message SHALL

a. Be for one-time-use only,
b. Comply with saml-core-2.0-os chapter 3.5[11],
c. Comply with saml-profiles-2.0-os chapter 5[12].

The *SourceID* of the Artifact SHALL be the crypthographic hash of the *entityID* declared in the metadata made available by the Identity Provider. The crypthographic hash function SHALL be known to resist up to date attacks.

The Authentication response message SHALL be signed using recommended cryptographic signature standards. The signature SHALL be validated by the relying party. The X.509 certificate used for signatures by the Verifier SHALL be issued by a trusted certificate service provider according to ZertES; SR 943.03 and listed by the Swiss Accreditation Service (SAS).

4.1.3.3 Artifact Resolve

The <ArtifactResolve> message SHALL be used by the Relying Party to resolve the artifact received with the <AuthenticationRequest> message to the SAML 2.0 Identity Assertion via the back-channel.

The <ArtifactResolve> message SHALL be cryptographically signed by the Relying Party and the Verifier SHALL validate the signature. The signature SHALL be asymmetric using X.509 certificates issued by a managed Certificate Authority (CA) that is operated according to documented processes detailed in a Certificate Policy (CP) and Certificate Practice Statement (CPS). The CA's processes should meet the requirements of class 1 certificates defined within the eCH-0048 PKI Certificate Classes standard (Version 2.0).

The signature SHALL either be validated with the public key of a pre-registered X.509 certificate, or the embedded certificate embedded. If the public key of the embedded certificate is used, the Verifier SHALL verify, that the certificate matches the pre-registered one.

4.1.3.4 Artifact Response

The <ArtifactResponse> message SHALL be used by the Verifier or Credential Service Provider to resolve the artifact received with the <ArtifactResolve> message to the SAML 2.0 Identity Assertion.

The Artifact response message SHALL be signed using recommended cryptographic signature standards. The signature SHALL be validated by the relying party. The X.509 certificate used for signatures by the Verifier SHALL be issued by a trusted certificate service provider according to ZertES; SR 943.03 and listed by the Swiss Accreditation Service (SAS).

4.1.3.5 Assertion

The SAML 2.0 Assertion SHALL be used by the Verifier or Credential Service Provider to convey the identity data of an authenticated Claimant/Subscriber to the requesting Relying Party.

The SAML 2.0 Assertion SHALL contain the following attributes:

---

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

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

a. First name with attribute name *http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname.*
b. Family name with attribute name http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname.
c. Gender with attribute name *gender*.
d. Date of birth with attribute name *dateofbirth*.

The attribute set MAY contain the GLN for healthcare professionals and assistants. If present, the GLN SHALL be contained in an <Attribute> element with the *Name* attribute set to “GLN”.

The <NameID> in the SAML 2.0 Assertion SHALL be persistent and SHALL be unique for the combination of the Subscriber, the Relying Party and the Identity Provider to impede cross application identification. The <NameID> SHALL be confidential and never presented to the Claimant, the User Agent or third party systems.

IDP MAY define a list of systems within its authority among which the <NAMEID> may be shared.

The SAML 2.0 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 2.0 Assertions SHALL only be considered as valid within the time limits specified in the <NotBefore> and <NotOnOrAfter> attributes. Assertions SHALL expire 5 minutes after the assertion has been issued.

The data types used in SAML 2.0 Assertions SHALL be according to W3C XML Schema.

SAML 2.0 Assertions SHOULD use audience restriction techniques to allow a Relying Party to recognize whether or not it is the intended target of an issued assertion.

The SAML 2.0 Assertions SHALL be cryptographically signed and the Relying Party SHALL validate the signature. The signature SHALL be asymmetric using X.509 certificates issued by a trusted certificate service provider according to ZertES; SR 943.03 and listed by the Swiss Accreditation Service (SAS).

4.1.3.6 Renew Request

Relying Parties MAY renew SAML Identity Assertions for the duration of the Verifier idle time after the assertion lifetime has expired without requiring a new authentication of the Claimant. To fulfill this requirement, the Verifier SHALL publish a web service compliant with the Web Services Trust standard (see fn. 10).

Relying Parties SHALL use an Identity Assertion of the Claimant in a <RequestSecurityToken> request as defined to the Web Services Security standard[13] and send it to the Verifier as SOAP version 1.1 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 (see fn. 13). The security timestamp element SHALL be covered by the XML signature.

The security timestamp element SHALL contain a <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 (see fn. 13). The security timestamp element SHALL contain an <Expires> element as described in chapter 10 of the Web Services Security specification (see fn. 13).

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 (see fn. 13). 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-

[13] OASIS Web Services Security: SOAP Message Security 1.1, February 2006

open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3". The binary token element MAY have an <Id> attribute.

The Renew Request SHALL be cryptographically signed and the Verifier SHALL validate the signature. The signature SHALL be asymmetric using X.509 certificates issued by a managed Certificate Authority (CA) that is operated according to documented processes detailed in a Certificate Policy (CP) and Certificate Practice Statement (CPS). The CA's processes should meet the requirements of class 1 certificates defined within the eCH-0048 PKI certificate classes standard (Version 2.0).

The Web Service security header of the SOAP envelope SHALL contain a signature element compliant 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. 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 <Id> attribute which is referenced in the key info element of the SOAP security header as described above.

The Verifier SHALL

a. Validate the signature of the request.
b. Verify the request timestamp, discard any message whose security semantics have passed their expiration and respond with a fault code (<MessageExpired>).
c. Verify the digest algorithm used with the request. The Verifier SHALL NOT accept deprecated digest algorithms, which do not resit up to date attacks.
d. Validate the signature of the previous Identity Assertion conveyed with the <RequestSecurityToken> request.

4.1.3.7 Renew Response

The Renew Response message SHALL be used by the Verifier or Credential Service Provider to convey an updated SAML Identity Assertion in the <RequestSecurityTokenResponse> according to the WS-Security Standard using SOAP version 1.1.

The Renew response message SHALL be signed using recommended cryptographic signature standards. The signature SHALL be validated by the relying party. The X.509 certificate used for signatures by the Verifier SHALL be issued by a trusted certificate service provider according to ZertES; SR 943.03 and listed by the Swiss Accreditation Service (SAS).

4.1.3.8 Logout Request

The <LogoutRequest> message SHALL be used by the Relying Party to notify the Verifier that a Claimant/Subscriber logged out in the Relying Party application and by the Verifier to notify Relying Parties that the session of a Claimant/Subscriber has been terminated.

SAML <LogoutRequest> messages SHALL include at least one <SessionIndex> as defined in Section 4.4.3.1 of the SAML Profiles 2.0 specification.

The <LogoutRequest> message SHALL be cryptographically signed by the sender and the receiver SHALL validate the signature. The signature SHALL either be validated with the public key of a pre-registered X.509 certificate, or the embedded certificate. If the public key of the embedded certificate is used, the Verifier SHALL verify, that the certificate matches the pre-registered one. The X.509-certificates used for signatures SHALL be issued by a managed Certificate Authority (CA) that is operated according to documented processes detailed in a Certificate Policy (CP) and Certificate Practice Statement (CPS). The CA's processes should meet the requirements of class 1 certificates defined within the eCH-0048 PKI Certificate Classes standard (Version 2.0).

Relying Parties SHALL sign the Logout Request message using X.509 certificates issued by a managed Certificate Authority (CA) that is operated according to documented processes detailed in a Certificate Policy (CP) and a Certificate Practice Statement (CSP). The CA's process should meet

the requirements of class 1 certificates defined within the eCH-0048 pKI Certificate Classes standard (version 2).

Verifier SHALL sign the Logout Request message. The X.509 certificate used for signatures by the Verifier SHALL meet recommended cryptographic standards and must follow certificate lifecycle best practices detailed in a certificate policy and certificate practice statement.

Receivers of signed Logout Request messages SHALL validate the signatures.

4.1.3.9 Logout Response

The <LogoutResponse> message SHALL be used by the Verifier or Relying Parties to confirm session termination.

Relying Parties SHALL sign the Logout Response message using X.509 certificates issued by a man-aged Certificate Authority (CA) that is operated according to documented processes detailed in a Certificate Policy (CP) and a Certificate Practice Statement (CSP). The CA's process should meet the requirements of class 1 certificates defined within the eCH-0048 pKI Certificate Classes standard (version 2).

Verifier SHALL sign the Logout Response message. The X.509 certificate used for signatures by the Verifier SHALL meet recommended cryptographic standards and must follow certificate lifecycle best practices detailed in a certificate policy and certificate practice statement.

Receivers of signed Logout Response messages SHALL validate the signatures.

4.2 OpenID Connect

Verifier and Credential Service Provider MAY provide trusted endpoints for Relying Parties implementing the OpenID Connect 1.0 Authorization Code Flow fulfilling the requirements defined in this section.

Other flows supported by OpenID Connect (i.e., Renew Flow, Hybrid or Implicit Flows) SHALL not be supported.

4.2.1 Sequences

4.2.1.1 User Authentication

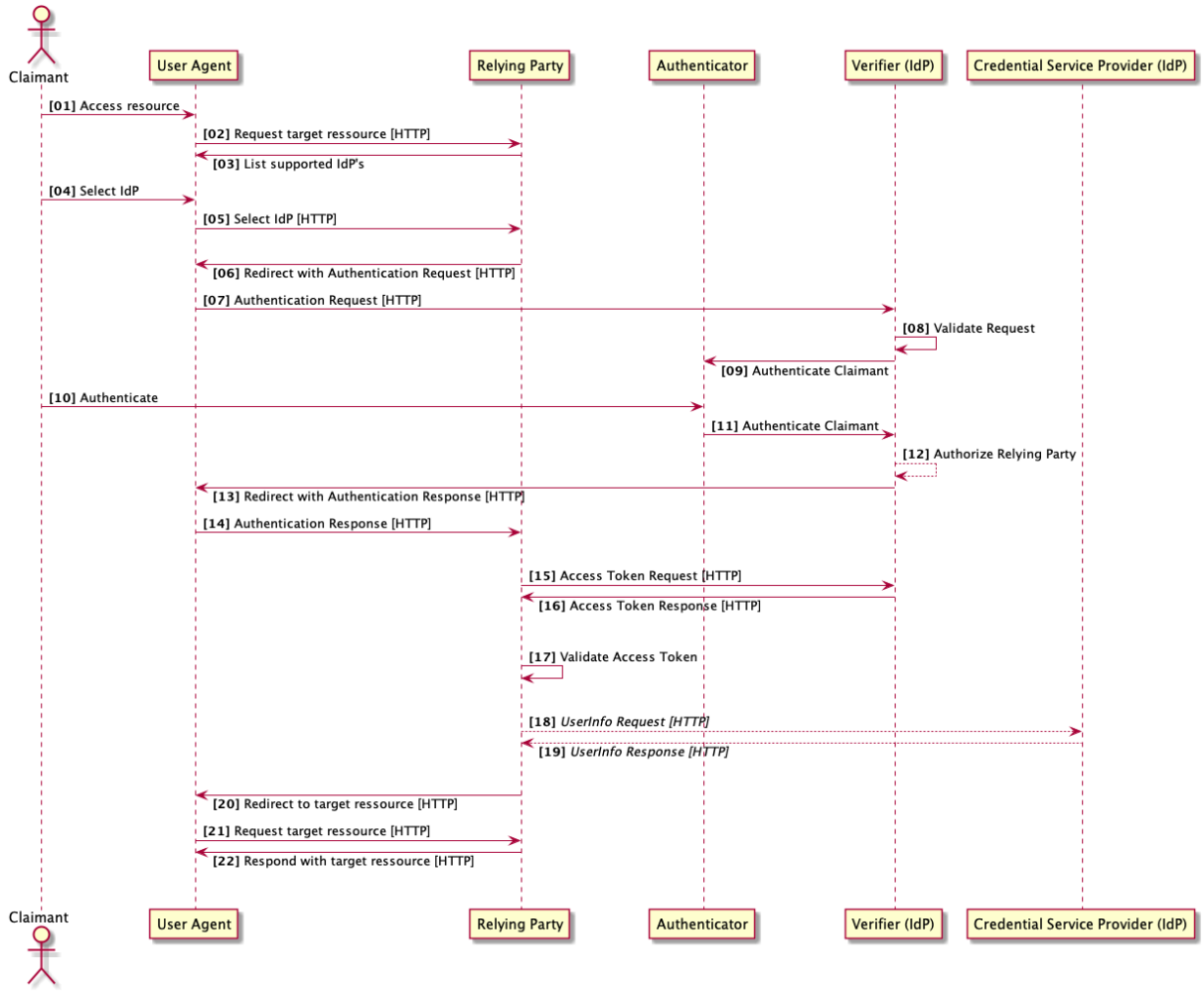

Figure 5: Authentication Sequence with OpenID Connect 1.0 Authorization Code Flow

SEQ	Description
01,02	The Claimant's user agent attempts to access a resource on the relying party.
03	The Relying Party presents the list of supported Verifiers to the Claimant.
04,05	The Claimant selects Verifier.

SEQ	Description
06	The Relying Party builds an Authentication Request containing the required request parameter and conveys it to the User Agent with a redirect to the authorization endpoint of the Verifier.
07	The User Agent sends the Authentication Request to the authorization endpoint via HTTP GET or POST protocol.
08	The Verifier determines whether the Claimant has an existing logon security context that meets the default or requested authentication policy requirements. If not, the Verifier interacts with the browser to challenge the Claimant to provide valid credentials.
09…11	The Verifier communicates with the Authenticator(s) to authenticate the Claimant. The Claimant provides valid credentials and the Verifier creates a local logon security context for the Claimant.
12	The Verifier presents a screen for the Claimant/Subscriber to authorize the Relying Party to retrieve the identity data. This step MAY be omitted if the Relying Party application is a confidential client as defined in the OAuth specification and the Claimant/Subscriber consent is stored in a policy or after the initial authorization.
13, 14	The Verifier creates an Authentication Response conveying the Authorization Code and sends the Authorization Response to the User Agent with a redirect to the Relying Party.
15	The Relying Party sends the Authentication Code to the Verifier in an Access Token Request using HTTP POST protocol and form serialization.
16	The Verifier identifies the Relying Party and sends an Access Token Response to the Relying Parties Redirection URI registered beforehand. The Access Token Response conveys an ID and an Access Token.
17	The Relying Party validates the ID Token and retrieves the Claimant's Subject Identifier.
18,19	Optionally the Relying Party uses the Access Token to retrieve user identity data using the OpenID Connect 1.0 UserInfo protocol.
20…22	The Relying Party returns the requested resource to the Claimant's user agent.

Table 6: Authentication Sequence with OpenID Connect 1.0 Authorization Code Flow

4.2.1.2 Logout

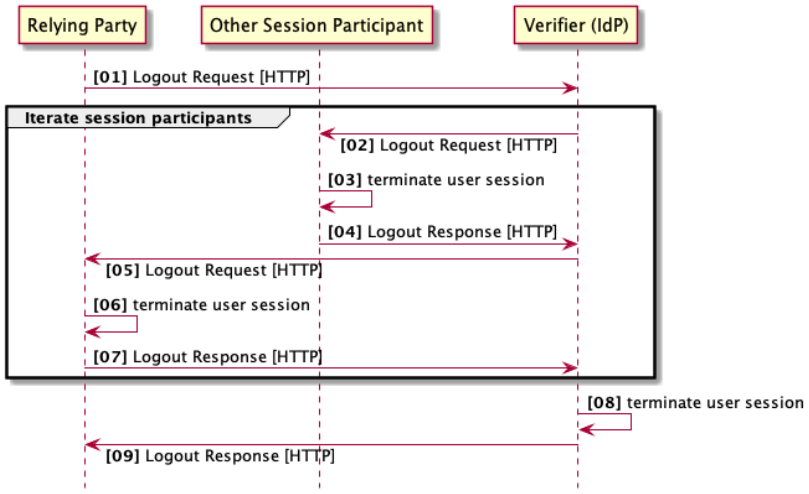

Figure 6: OpenID Connect Logout Sequence

SEQ	Description
01	The Claimant initiates a logout in the user agent of the Relying Party application. The Relying Party redirects the user agent with a Logout Request message to the Verifier Logout URI.
02	The Verifier determines all other session participants and sends a Logout Request message on the backchannel via HTTP to the Logout URI of all Relying Parties joining the same session.

SEQ	Description
03, 04	The other Relying Parties joining the same session terminate their user session and responds a Logout Response message to the Verifier.
05	The Verifier determines sends a Logout Request message on the backchannel via HTTP to the Logout URI of the Relying Party.
06, 07	The Relying Party terminates the user session and responds a Logout Response message to the Verifier.
08, 09	The Verifier terminates the IdP session and responds to the initial Logout Request with a Logout Response using HTTP.

Table 7: OpenID Connect Logout Sequence

4.2.2 Protocol Requirements

4.2.2.1 Front-channel Communication

The User Agent and the Verifier SHALL communicate through an authenticated protected channel using TLS 1.2 or higher. The Verifier SHALL identify and authenticate itself with X.509 certificates which are issued by a class 2 TLS certificate issued by a trusted certificate service provider according to ZertES; SR 943.03 and listed by the Swiss Accreditation Service (SAS).

Relying Parties and Authenticators which communicate with the Verifier and Credential Service Provider through an intermediary user agent SHALL use digital signatures for message level authentication. The X.509 certificates used for signatures SHALL be issued by a managed Certificate Authority (CA) that is operated according to documented processes detailed in a Certificate Policy (CP) and Certificate Practice Statement (CPS). The CA's processes SHALL meet the requirements of class 1 certificates defined within the eCH-0048 PKI Certificate Classes standard (Version 2.0).

Relying Parties which fulfill the requirements of confidential clients of the OAuth 2.0 specification SHALL use digital signatures for message level authentication.

4.2.2.2 Back-channel Communication

The Verifier and the Credential Service provider SHALL communicate with Relying Parties through an authenticated and protected back-channel using TLS 1.2 or higher for access token and user info requests and responses. The Verifier SHALL identify and authenticate itself with class 2 X.509 certificates issued by a trusted certificate service provider according to ZertES; SR 943.03 and listed by the Swiss accreditation service (SAS).

Relying Parties SHALL which fulfill the requirements of OAuth 2.0 confidential clients, SHALL use message level authentication (e.g., digital signature) to authenticate. Relying Parties SHALL use X.509 certificates issued by a managed Certificate Authority (CA) that is operated according to documented processes detailed in a Certificate Policy (CP) and Certificate Practice Statement (CPS) to identify and authenticate themselves for access token and user info requests. The CA's processes should meet the requirements of class 1 certificates defined within the eCH-0048 PKI Certificate Classes standard (Version 2.0).

The Verifier and the Credential Service Provider SHALL NOT use redirects through an intermediary user agent (e.g., Web Browser) to send requests to Relying Parties.

4.2.2.3 Client Authentication

If the Relying Parties provides confidential clients, the clients SHALL authenticate when performing Access Token Requests using the *private_key_jwt* option defined in Section 9 of the OpenID Connect Core 1.0 specification[14].

[14] OpenID Connect Core 1.0 incorporating errata set 1, November 2014.

4.2.3 Messages

4.2.3.1 Authentication Request

The Authentication Request message SHALL be used by the Relying Party to initiate the authentication sequence. The Authentication Request message SHALL be compliant with an OAuth 2.0 Authentication Request message.

Relying Parties which fulfill the requirements of confidential clients[15] SHALL sign the Authentication Request message using JSON Web Signature[16]. The signature SHALL be asymmetric using X.509 certificates issued by a managed Certificate Authority (CA) that is operated according to documented processes detailed in a Certificate Policy (CP) and Certificate Practice Statement (CPS). The CA's processes should meet the requirements of class 1 certificates defined within the eCH-0048 PKI Certificate Classes standard (Version 2.0).

The Authentication Request SHALL contain the following parameters:

a. *scope* – The value SHALL be *openid*.
b. *response_type* – The value SHALL be *code*.
c. *client_id* – The value SHALL be the Client Identifier the Relying Party was registered with at the Verifier.
d. *redirect_uri* – SHALL convey the redirection URI the Access Token Response SHALL be sent to. Its value must match one of the redirection URI the Relying Party was registered at the Verifier.
e. *state* – SHALL convey an opaque value used to maintain the state between the request and the response to mitigate Cross-Site Forgery attacks.
f. *nonce* – SHALL convey an opaque string passed through from the Authentication Request to the ID Token to mitigate replay attacks.
g. *code_challenge* – code challenge derived from the code verifier using the code challenge method as defined in PKCE[17]
h. *code_challenge_method* – code challenge method indicator defined in PKCE (fn. 17). Its value must be S256.

The Verifier SHALL validate the Access Token Request as follows:

i. Identify the client using the *client_id*.
j. Verify the signature of the request, if the Relying Party is registered as a confidential client.
k. Verify that a secure cryptographic algorithm is applied.
l. Authenticate the Relying Party, if the client application is registered as a confidential client.
m. Validate the signature according to JSON Web Signature (see fn. 16) using the algorithm specified in the JWT *alg* Header Parameter.

4.2.3.2 Authentication Response

The Authentication Response message SHALL be used by the Verifier as response to the Authentication Request message to convey the authorization code after authenticating the Claimant/Subscriber. The Authentication Response message SHALL be compliant with an OAuth 2.0 Authentication Response message.

The Authentication Response SHALL contain the following parameters:

a. *code* – SHALL be an OAuth 2.0 compliant authorization code.

---

15 The OAuth 2.0 Authorization Framework, RFC 6749, October 2012

16 JSON Web Signature (JWS), RFC 7515, May 2015.

17 RFC 7636: Proof Key for Code Exchange by OAuth Public Clients, https://www.rfc-editor.org/rfc/rfc7636

b. *state* – SHALL match the state parameter value of the Authentication Request.

In case of an error the Verifier SHALL respond a HTTP Error as defined in Section 3.1.2.6 of the OpenID Connect Core 1.0 specification (see fn. 14).

The authentication response message SHALL be signed using recommended cryptographic signature standards. The signature SHALL be validated by the relying party. The X.509 certificate used for signatures by the Verifier SHALL be issued by a trusted certificate service provider according to ZertES; SR 943.03 and listed by the Swiss Accreditation Service (SAS).

4.2.3.3 Access Token Request

The Access Token Request message SHALL be used by the Relying Party to resolve the authorization code to the Access and ID Token. The Access Token Request message SHALL be send via the back-channel. The Access Token Request message SHALL be compliant with an OAuth 2.0 Access Token Request message.

Relying Parties which fulfill the requirements of confidential clients (see fn. 15) SHALL sign the Access Token Request message using JSON Web Signature (see fn. 16). The signature SHALL be asymmetric using X.509 certificates issued by a managed Certificate Authority (CA) that is operated according to documented processes detailed in a Certificate Policy (CP) and Certificate Practice Statement (CPS). The CA's processes should meet the requirements of class 1 certificates defined within the eCH-0048 PKI Certificate Classes standard (Version 2.0).

The Access Token Request SHALL contain the following parameters:

a. grant_type – The value SHALL be authorization_code.
b. code – SHALL be the OAuth 2.0 compliant authorization code retrieved with the Authentication Response.
c. redirect_uri – SHALL convey the redirection URI the Access Token Response SHALL be sent to. Its value must match the redirection URI sent with the Authentication Request.
d. code_verifier – The code verifier value as defined in PKCE (fn. 17).

The Verifier SHALL validate the Access Token Request as follows:

e. Identify the client using the client_id.
f. Verify the signature of the request, if the Relying Party is registered as a confidential client, i.e. verify that a secure cryptographic algorithm is applied compliant with the JSON Web Signature (see fn. 16) specification.
g. Authenticate the Relying Party, if the client application is registered as a confidential client.
h. Verify that the authorization code was issued to the Relying Party in response to an Authentication Request.
i. Verify that the authorization code was not used before.
j. Verify that the value of the *redirect_uri* parameter send with the Access Token Request matches the one send with the Authentication Request.
k. Verify that the value of the *redirect_uri* parameter send with the Access Token Request matches one of the redirection URIs registered for the Relying Party.
l. Verify that the *code-verifier* matches the *code_challenge* send with the authentication request respecting the S256 code challenge method.

4.2.3.4 Access Token Response

The Access Token Response message SHALL be used by the Verifier convey the Access Token and the ID Token to the Relying Party in response the Access Token Request. The Access Token Response message SHALL be send via the back-channel. The Access Token Response message SHALL be compliant with an OAuth 2.0 Access Token Response message.

The Access Token Response SHALL contain the following parameters:

a. *token_type* – The value SHALL be *Bearer.*

b. *expires_in* – The Token lifetime in seconds. The value SHALL be equal to *300* (5 minutes).

c. *access_token* – The value SHALL be an OAuth 2.0 compliant access token.

d. *id_token* – The value shall be an Identity Token as defined below.

In case of an error the Verifier SHALL respond a HTTP Error as defined in Section 3.1.3.4 of the OpenID Connect Core 1.0 specification (see fn. 14).

The access token response message SHALL be signed using recommended cryptographic signature standards. The signature SHALL be validated by the relying party. The X.509 certificate used for signatures by the Verifier SHALL be issued by a trusted certificate service provider according to ZertES; SR 943.03 and listed by the Swiss Accreditation Service (SAS).

4.2.3.5 Identity Token

The Identity Token SHALL be used by the Verifier to convey the Subject Identifier to the Relying Party. The Identity Token SHALL be compliant with the JSON Web Token[18] and OpenID Connect Core 1.0 specification (see fn. 14).

Identity Tokens SHALL be cryptographically signed using JSON Web Signature (see fn. 16) and the Relying Party SHALL validate the signature. The X.509 certificate used for signatures by the Verifier SHALL be issued by a trusted certificate service provider according to ZertES; SR 943.03 and listed by the Swiss Accreditation Service (SAS).

The Identity Token SHALL contain the following parameters:

a. *iss* – The value SHALL be a unique identifier of the Issuer Credential Service Provider as URL.

b. *sub* – The Subject Identifier of the Claimant/Subscriber.

c. *aud* – The value SHALL be the Client Identifier the Relying Party is registered at the Verifier.

d. *exp* – The time restricting the lifetime of the token lifetime. The value SHALL be equal to the current time plus 5 minutes.

e. *iat* – The time the token was issued by the Verifier.

f. *nonce* – The value SHALL match the *nonce* value of the Authentication Request.

g. *jti* – The value shall be a unique identifier of the ID Token.

The Subject Identifier attribute SHALL be persistent and SHALL be unique for the combination of the Subscriber, the Relying Party and the Identity Provider to impede cross application identification. The Subject Identifier SHALL be confidential and never presented to the Claimant or third party systems.

IDP MAY define a list of systems within its authority among which the Subject Identifier attribute may be shared.

The Identity Token MAY contain a session identifier in a *sid* attribute, if the Identity Provider supports per session logout[19].

The Identity Token MAY contain other claims which SHALL be ignored by the Relying Party.

The Relying Parties SHALL validate Identity Tokens as follows:

h. Verify that the unique identifier of the Issuer matches the one registered for the Verifier.

i. Verify that the value of the *aud* parameter matches the Client Identifier of the Relying Party.

j. Validate the signature according to JSON Web Signature (see fn. 16) using the algorithm specified in the JWT *alg* Header Parameter.

k. Verify that the signature algorithm matches the algorithm configured for the Verifier.

---

[18] JSON Web Token (JWT), RFC 7519, May 2015.

[19] OpenID Connect Back-Channel Logout 1.0 - draft 06, August 2020

l. Verify that the Identity Token is not expired and the current time is later or equal to the time the token was issued by the Verifier.

m. Verify that a *nonce* claim is present and its value matches the one that was sent in the Authentication Request.

4.2.3.6 User Info Request

The UserInfo Request message SHALL be used by the Relying Party to retrieve identity data of the Claimant/Subscriber from the Credential Service Provider via the back-channel. The UserInfo Request message SHALL be compliant to the OpenID Connect 1.0 UserInfo Request message.

Relying Parties which fulfill the requirements of confidential clients (see fn. 15) SHALL sign the UserInfo Request message using JSON Web Signature (see fn. 16). The signature SHALL be asymmetric using X.509 certificates issued by a managed Certificate Authority (CA) that is operated according to documented processes detailed in a Certificate Policy (CP) and Certificate Practice Statement (CPS). The CA's processes should meet the requirements of class 1 certificates defined within the eCH-0048 PKI Certificate Classes standard (Version 2.0).

The Relying Party SHALL send the Access Token in the HTTP Authorization header field as Bearer Token as defined in The OAuth 2.0 Authorization Framework: Bearer Token Usage[20].

The Credential Service Provider SHALL validate the User Info Request as follows:

a. Validate the signature according to JSON Web Signature [24] using the algorithm specified in the JWT *alg* Header Parameter.

b. Verify that the signature algorithm matches the algorithm configured for the Relying Party at the Credential Service Provider.

4.2.3.7 UserInfo Response

The UserInfo Response message SHALL be used by the Credential Service Provider to respond with the identity data of the Claimant/Subscriber to UserInfo Requests from the Relying Party using back-channel communication. The UserInfo Response message SHALL be a JSON Web Token (JWT) compliant to the OpenID Connect 1.0 UserInfo Response message.

The UserInfo Response SHALL contain the followong parameters:

a. *first_name* – The first name of the Claimant/Subscriber.

b. *family_name* – The family name of the Claimant/Subscriber.

c. *gender* – The Claimants/Subscribers coded gender with the value from the value set EprGender (2.16.756.5.30.1.127.3.10.1.25).

d. *birthdate* – The Claimants/Subscribers date of birth as ISO 8601 formatted string.

If the Identity Provider delivers the GLN of healthcare professionals or assistants, the UserInfo Response SHALL contain a *gln* parameter conveying the GLN of healthcare professionals and assistants.

Credential Service Provider MAY provide other identity claims as defined in the OpenID Connect 1.0 Core specification (see fn. 14).

In case of an error the Credential Service Provider SHALL respond a HTTP Error as defined in Section 5.3.3 of the OpenID Connect Core 1.0 specification (see fn. 14).

The UserInfo response message SHALL be signed using recommended cryptographic signature standards. The signature SHALL be validated by the relying party. The X.509 certificate used for signatures by the Verifier SHALL be issued by a trusted certificate service provider according to ZertES; SR 943.03 and listed by the Swiss Accreditation Service (SAS).

[20] The OAuth 2.0 Authorization Framework: Bearer Token Usage, RFC 6750, October 2012

4.2.3.8 Logout Request

The Logout Request message SHALL be used by Relying Parties and Verifier to initiate session termination at the receiver. The Logout Request message send by the Relying Party to the Verifier to initiate the logout sequence SHALL be compliant with the OpenID Connect RP-Initiated Logout 1.0 specification[21] and the Logout Request Message send by the Verifier to the Relying Parties sharing the same session SHALL be compliant with Logout Request message defined in the OpenID Connect back-channel Logout specification (see fn. 19) with the requirements defined in this section.

Logout Request message send by the Relying Party to the Verifier to initiate the logout sequence SHALL contain a JWT with the following parameters:

a. *id_token_hint* – SHALL convey the Identity Token previously issued by the Verifier.
b. *state* – SHALL convey an opaque value used to maintain the state between the request and the response to mitigate Cross-Site Forgery attacks.

The JWT MAY contain other claims which SHALL be ignored by the Verifier.

Relying Parties which fulfill the requirements of confidential clients (see fn. 15) SHALL sign the Log-out Request message using JSON Web Signature (see fn. 16). The signature SHALL be asymmetric using X.509 certificates issued by a managed Certificate Authority (CA) that is operated according to documented processes detailed in a Certificate Policy (CP) and Certificate Practice Statement (CPS). The CA's processes should meet the requirements of class 1 certificates defined within the eCH-0048 PKI Certificate Classes standard (Version 2.0).

The Verifier SHALL validate Logout Requests as follows:

c. Verify that the Identity Token was issued by the Verifier for the requesting client and user.
d. Verify the signature of the Request Message, if the Relying Party was registered as confidential client.

The Logout Request send by the Verifier to the Relying Parties sharing the same session SHALL contain a JWT with the following parameters:

e. iss – The value SHALL be a unique identifier of the Verifier which issued the initial ID Token as URL.
f. aud – The value SHALL be the Client Identifier the Relying Party is registered at the Verifier.
g. iat – The time the token was issued by the sender.
h. jti – The value shall be the unique identifier of the ID Token.
i. events – JSON object which SHALL contain the value http://schemas.openid.net/event/backchannel-logout to declare the token to be a logout request token.

The JWT MAY contain a session identifier in the *sid* attribute, if the Verifier supports per session logout (see fn. 19).

The JWT MAY contain other claims which SHALL be ignored by the Relying Party.The Relying Party SHALL validate Logout Requests as follows:

j. Verify that the unique identifier of the Issuer matches the one registered for the Verifier.
k. Verify that the value of the aud parameter matches the Client Identifier of the Relying Party.
l. Validate the signature according to JSON Web Signature [24] using the algorithm specified in the JWT alg Header Parameter.
m. Verify that the current time is later or equal to the time the the Logout Request was issued by the Verifier.

Relying Parties SHALL sign the Logout Request message using X.509 certificates issued by a managed Certificate Authority (CA) that is operated according to documented processes detailed in a Certificate Policy (CP) and a Certificate Practice Statement (CSP). The CA’s process should meet

[21] OpenID Connect RP-Initiated Logout 1.0 - draft 01, August 2020

the requirements of class 1 certificates defined within the eCH-0048 pKI Certificate Classes standard (version 2).

Verifier SHALL sign the Logout Request message. The X.509 certificate used for signatures by the Verifier SHALL meet recommended cryptographic standards and must follow certificate lifecycle best practices detailed in a certificate policy and certificate practice statement.

Receivers of signed Logout Request messages SHALL validate the signatures.

4.2.3.9 Logout Response

The Logout Response message SHALL be used by Relying Parties and Verifier to confirm session termination at the sender. The Logout Response message SHALL be compliant with Logout Response message defined in the OpenID Connect back-channel Logout specification [25] with the requirements defined in this section.

The receiver SHALL respond to a Logout Request as follows:

a. If the logout succeeded, the receiver SHALL respond with HTTP 200 (OK).
b. If the logout request was invalid, the receiver SHALL respond with HTTP 400 (Bad Request).
c. If the local logout succeeded but some downstream logouts have failed, the receiver SHALL respond with HTTP 504 (Gateway Timeout).
d. If the logout failed, the receiver SHALL respond with HTTP 501 (Not Implemented).

Relying Parties SHALL sign the Logout Response message using X.509 certificates issued by a man-aged Certificate Authority (CA) that is operated according to documented processes detailed in a Certificate Policy (CP) and a Certificate Practice Statement (CSP). The CA's process should meet the requirements of class 1 certificates defined within the eCH-0048 pKI Certificate Classes standard (version 2).

Verifier SHALL sign the Logout Response message. The X.509 certificate used for signatures by the Verifier SHALL meet recommended cryptographic standards and must follow certificate lifecycle best practices detailed in a certificate policy and certificate practice statement.

Receivers of signed Logout Response messages SHALL validate the signatures.

5 Appendix

5.1 List of tables

5.2 List of figures

5.3 Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CC	Common Criteria
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
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 Target of Evaluation
OE	Security Objectives for the Operational Environment

Acronym	Definition
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PP	Protection Profile
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
SQL	Structured Query Language
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	Target of Evaluation Security Functionality
XML	Extensible Markup Language
XPATH	XPath is a language for addressing parts of an XML document
XSS	Cross-Site Scripting

5.4 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 output.
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 (see fn. 1).
Assertion Data	A data object from a Verifier or Credential Service Provider 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 Target of Evaluation presumably places value upon. (CC Part 1)
Authentication	Provision of assurance in the identity of an entity (see fn. 1).
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) (see fn. 1);

Term	Definition
	something an entity knows (e.g., password, PIN); something an entity is (e.g., biometric characteristic); something an entity typically does (e.g., behavior pattern).
Authenticator	Something that the Claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the Claimant's identity.
Authoritative Source	Repository which is recognized as being an accurate and up-to-date source of information (see fn. 1).
back-channel	Communication between two systems that relies on a direct connection (allowing for standard protocol-level proxies), without using redirects through an intermediary such as a browser. This can be accomplished using HTTP requests and responses.
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)
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 (see fn. 1). An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber (see fn. 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 (see fn. 1).
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	Communication between two systems that relies on redirects through an intermediary such as a browser.
Identifier	One or more attributes that uniquely characterize an entity in a specific context (see fn. 1).
Identity	Set of attributes related to an entity (see fn. 1).
Inter TSF Transfers	Communicating data between the Target of Evaluation and the security functionality of other trusted IT products. (CC Part 1)
Internal Communication Channel	Communication channel between separated parts of the Target of Evaluation. (CC Part 1)
Object	Passive entity in the Target of Evaluation, 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.

Term	Definition
	(CC Part 1)
Operational environment	Environment in which the Target of Evaluation is operated. (CC Part 1)
Protection Profile	Implementation-independent statement of security needed for a Target of Evaluation 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 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
SAML Artifact	A small, fixed-size, structured data object pointing to a typically larger, variably-sized SAML protocol message. (SAML Glossary)
Secret/Private Credential	Credentials that cannot be disclosed by a Credential Service Provider or disseminate to the public because the contents can be used to compromise the authenticator.
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 Protection Profile 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 Target of Evaluation is intended to address This statement consists of a combination of: threats to be countered by the Target of Evaluation and its operational environment, the organizational security policies enforced by the Target of Evaluation and its operational environment, and the assumptions that are upheld for the operational environment of the Target of Evaluation (CC Part 1).
Subject	Active entity in the Target of Evaluation that performs operations on objects (CC Part 1).
Target of Evaluation	Set of software, firmware and/or hardware possibly accompanied by guidance (CC Part 1).
Target of Evaluation	Assessment of a Target of Evaluation against defined criteria (CC Part 1).
Target of Evaluation Security Functionality	Combined functionality of all hardware, software, and firmware of a Target of Evaluation that must be relied upon for the correct enforcement of the SFRs (CC Part 1).
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 Relying Parties and Verifier and Credential Service Provider SHALL be protected accordingly.
TSF Data	Data for the operation of the Target of Evaluation upon which the enforcement of the SFR relies (CC Part 1).

Term	Definition
TSF Interface	Means by which external entities (or subjects in the Target of Evaluation 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).