SwissSign Group

# SwissID White Paper

SwissSign Group AG
Sägereistrasse 25
CH-8152 Glattbrugg
swissid.ch

Inhaltsverzeichnis

**1 Ziel und Zweck ... 3**
**2 Begriffe ... 3**
2.1 Das Ökosystem von SwissID ... 3
2.2 Weitere Begriffsdefinitionen ... 4
**3 Funktionen von SwissID ... 6**
3.1 Vertrauensstufen von SwissID: die Funktion «Einfaches Einloggen» ... 7
3.2 Austausch von Attributen: Die Funktion «Informationen freigeben» ... 9
**4 Sicherheitsrelevante Leitlinien für das Ökosystem von SwissID ... 10**
**5 Entwicklung ... 11**
5.1 Produktlebenszyklus ... 11
5.2 Entwicklungsmethodik ... 12
**6 Data Governance und Datenschutz ... 12**
6.1 Rechtsbeziehungen im SwissID Ökosystem ... 12
6.2 Verhältnis IdP –Onlinedienstanbieter ... 13
6.3 Regeln und Prinzipien des Datenschutzes von SwissID ... 14
**7 Technische und organisatorische Massnahmen zur Datensicherheit ... 15**
7.1 Zugangskontrolle (Art.9 lit. a VDSG) ... 15
7.2 Personendatenträgerkontrolle (Art.9 lit. b VDSG) ... 15
7.3 Transportkontrolle (Art.9 lit. c VDSG) ... 15
7.4 Bekanntgabekontrolle (Art.9 lit. d VDSG) ... 16
7.5 Speicherkontrolle (Art.9 lit. e VDSG) ... 16
7.6 Benutzerkontrolle (Art.9 lit. f VDSG) ... 16
7.7 Zugriffskontrolle (Art.9 lit. g VDSG) ... 17
7.8 Eingabekontrolle (Art.9 lit. h VDSG) ... 17
7.9 Verfügbarkeitskontrolle ... 17
7.10 Trennungskontrolle ... 18

# 1 Ziel und Zweck

Die Nutzung von digitalen Dienstleistungen wird immer beliebter, die Komplexität, die sich dadurch für die Nutzer ergeben auch. Nicht nur müssen sie sich jedes Mal neu registrieren, sondern auch eine grosse Anzahl von Benutzernamen und Passwörtern verwalten. Um der Komplexität entgegenzuwirken, verwenden Nutzer oft die identischen Benutzernamen und dieselben eher einfachen Passwörter auf unterschiedlichen Internetseiten, was aus Sicherheitssicht durchaus heikel ist. Für gewisse Geschäftsvorgänge im Netz ist eine digitale Identität von grossem Nutzen. An dieser Stelle setzt SwissID an und bietet eine einheitliche, sichere und datenschutzkonforme digitale Identität für vertrauenswürdige und rechtskonforme digitale Geschäftsprozesse.

Das vorliegende White Paper hat zum Ziel die sicherheitsrelevanten Aspekte von SwissID darzulegen. Zielpublikum sind sowohl Onlinedienstanbieter als auch SwissID Inhaber. Die Ausführungen betreffen sowohl SwissID-Funktionen (sicherheitsrelevante Grundsätze, Ausführungen sicherheitsrelevanter Natur, Infrastruktur und Plattformen) als auch Aussagen zum Datenschutz im Zusammenhang mit der Nutzung von SwissID.

Die Ausführungen in diesem White Paper beziehen sich auf den aktuellen Stand der Technik und Diskussionen über die relevanten gesetzlichen Anforderungen z.B. des E-ID-Gesetzes (Oktober 2018) und stehen unter dem Vorbehalt der Anpassungen an entsprechende Entwicklungen.

# 2 Begriffe

## 2.1 Das Ökosystem von SwissID

Um die weiteren Ausführungen in diesem White Paper einfacher nachzuvollziehen, werden nachfolgend die wichtigen Teilnehmer des Ökosystems von SwissID kurz illustrativ dargestellt.

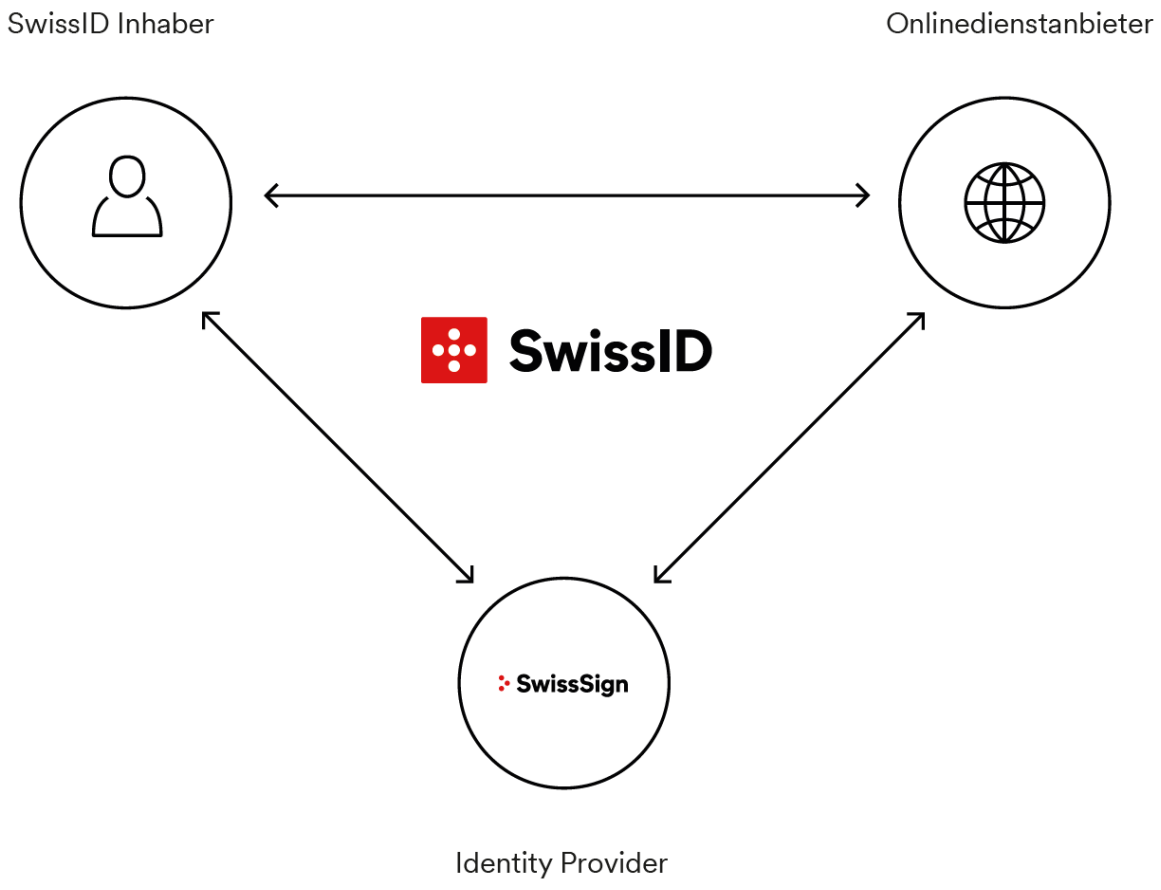


*Abbildung 1: Das Ökosystem von SwissID*

- **SwissID Inhaber (IdO):** Privater Anwender[1], der SwissID zum Einloggen bei Schweizer Onlinediensten einsetzt und dabei die vollständige Kontrolle über seine Daten behält.
- **Identity Provider (IdP):** Der Erbringer von elektronischen Identitätsdienstleitungen. In diesem Dokument die SwissSign Group AG als Herausgeber von SwissID. Der Identity Provider verständigt sich vertraglich mit dem Onlinedienstanbieter auf die Nutzung von SwissID-Schnittstellen (API).
- **Onlinedienstanbieter (Relying Party):** Relying Party d.h. Betreiberin/Onlinedienstanbieterin von SwissID verwendenden Diensten.

### 2.2 Weitere Begriffsdefinitionen

| Begriff | Definition |
|---|---|
| Authentifizierungsmittel | Das Authentifizierungsmittel bezeichnet die Methode mit welcher sich der SwissID Inhabergegenüber Onlinedienstanbietern authentisiert z.B. Passwort, SMS-Code, SwissID-App etc. Es können, je nach Anforderung des Onlinedienstanbieters auch eine Kombination mehrerer Mittel erforderlich sein. |
| DSG | Bundesgesetz über den Datenschutz (SR 235.1). |
| VDSG | Verordnung zum Bundesgesetz über den Datenschutz (SR 235.11). |
| E-ID Gesetz | Entwurf des Bundesgesetzes über anerkannte elektronische Identifizierungseinheiten (noch nicht in Kraft). |
| Erweiterte Attribute | Personendaten, welche gemäss E-ID-Gesetz nicht der Basisidentität zuzuordnen sind. Darunter fallen Attribute wie u.a. die E-Mail-Adresse, die Mobilnummer und die Korrespondenzadresse. |
| FINMA | Eidgenössische Finanzmarktaufsichtsbehörde |
| GWG | Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (SR 955.0). |
| Identitätsattribute | Personendaten, welche gemäss E-ID-Gesetz dem SwissID Inhaber zuzuordnen sind. Darunter fallen je nach Sicherheitsniveau gemäss E-ID-Gesetz der amtliche Name, Vornamen, Geburtsdatum, Geschlecht, Geburtsort und die Staatsangehörigkeit. |
| Level of Trust (LoT) | Definiert die Vertrauensstufe zum SwissID Inhaber bestehend aus der Kombination der «Qualität der Authentifizierung (QoA) und der Qualität der Registrierung (QoR). |
| Mobile ID | Mobile ID ist ein Authentifikationsmittel basierend auf einem Hardware Crypto Token auf der SIM Karte des SwissID Inhabers. |
| NIST | Das National Institute of Standards and Technology definiert einen allgemein anerkannten Richtlinienrahmen im Bereich der Cyber-Security. |
| Ökosystem | Das Ökosystem von SwissID besteht aus diversen Rollen wie Identity Provider (IdP), SwissID Inhaber, Onlinedienstanbieter, Vermittler etc. |
| Qualität der Authentifizierung (QoA) | Die QoA definiert die Qualität der Authentifizierung in Bezug auf das Authentifizierungsmittel, das verwendet wurde. |
| Qualität der Registrierung (QoR) | Die QoR bestimmt das Sicherheitsniveau bei der Registrierung bzw. der Erhebung der E-ID-Identitätsattributen. Die bei SwissID verwendeten QoR lehnen sich an die aktuellen Definitionen im Rahmen von E-ID an. |

[1] In diesem Dokument wird auf die explizite Nennung der weiblichen Formen verzichtet, da sie in der männlichen Form mitgemeint sind.

| | |
|---|---|
| User-Self-Management | Das Online-Kundenportal eines SwissID Inhabers. |
| Universally Unique Identifier (UUID) | Die UUID bezeichnet eine eineindeutige Kennung des SwissID Inhabers gegenüber einem Onlinedienst. |
| Verifikationslevel | Das Verifikationslevel wird bei erweiterten Attributen angewandt. Es entspricht der QoR bei Identitätsattributen. |
| ZertES | Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (SR 943.03). |

## 3 Funktionen von SwissID

SwissID umfasst drei wesentliche Funktionen im Zusammenhang mit digitalen Geschäftstransaktionen:

- «Einfaches Einloggen»
- «Informationen freigeben»
- «Geschäfte abschliessen»

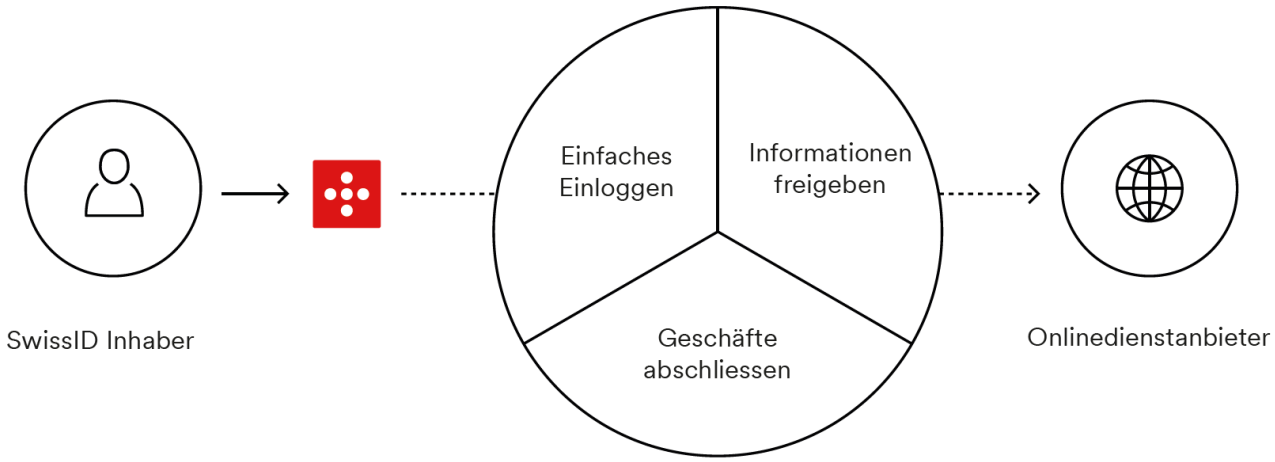


*Abbildung 2: Die Funktionen von SwissID*

Die nachfolgenden Ausführungen beziehen sich auf die Funktionen «Einfaches Einloggen» und «Informationen freigeben». Die Funktion «Geschäfte abschliessen» befindet sich derzeit noch im Aufbau und wird Anfang 2019 zur Verfügung stehen.

Eine zentrale Rolle bei den Funktionen «Einfaches Einloggen» und «Informationen freigeben» spielen die Attribute. Zum besseren Verständnis wird nachfolgend kurz erklärt, was unter Attributen verstanden wird und welche Attributsklassen es im Zusammenhang mit der Nutzung von SwissID gibt.

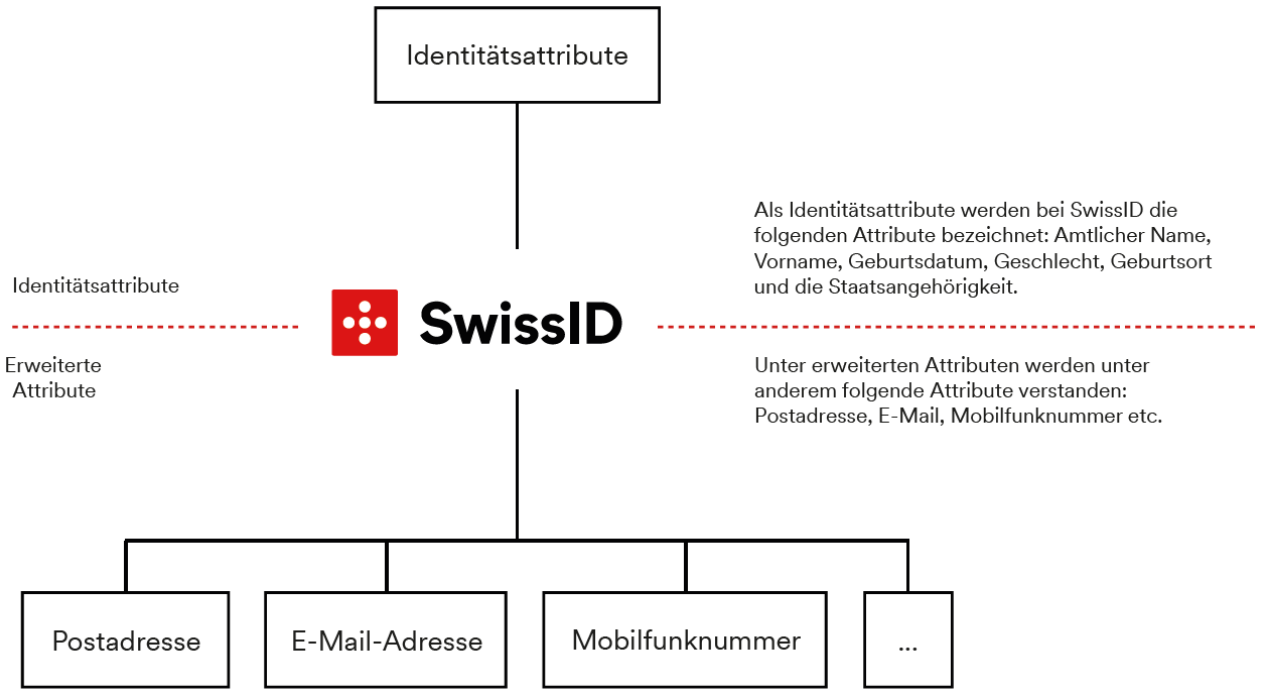


*Abbildung 3: Identitäts- und erweiterte Attribute von SwissID*

Mit der Erfassung der Identitätsattribute beim Anlegen eines neuen SwissID-Kontos sowie durch den Schutz mittels einer geeigneten Authentifikation wird sichergestellt, dass nur der tatsächliche Identitätsinhaber ein SwissID-Konto erstellen und anschliessend nutzen kann. Abhängig vom Verwendungszweck und den anzuwendenden regulatorischen Vorschriften kann eine Identifikation des SwissID Inhabers und eine Authentifikation auf verschiedenen Vertrauensstufen notwendig sein.

Der SwissID Inhaber ist gemäss den AGB von SwissID verpflichtet, bei der Registrierung und anderen Nutzungshandlungen vollständige und wahrheitsgemässe Angaben zu machen, alle Angaben über das Online-Kundenportal auf www.swissid.ch aktuell zu halten und Fehler umgehend zu berichtigen. Liegen die Identitätsattribute bereits auf einem höheren, geprüften Verifikationslevel vor und werden diese nun durch den SwissID Inhaber angepasst, müssen diese Änderungen zwingend nochmals durch einen geeigneten Verifikationsmechanismus überprüft werden, z.B. durch eine zertifizierte Drittpartei.

### 3.1 Vertrauensstufen von SwissID: die Funktion «Einfaches Einloggen»

Im Zusammenhang mit der Nutzung von SwissID werden verschiedene Vertrauensstufen unterschieden. Diese definieren sich entlang der beiden Dimensionen «Qualität der Authentifizierung» (QoA) und der «Qualität der Registrierung» (QoR). Welche Vertrauensstufe für die Nutzung eines Onlinedienstes notwendig ist, wird im Sinne einer Mindestanforderung durch den jeweiligen Onlinedienstanbieter definiert. Der Onlinedienstanbieter erhält nur die für seine Dienstleistung erforderlichen Identitätsdaten.

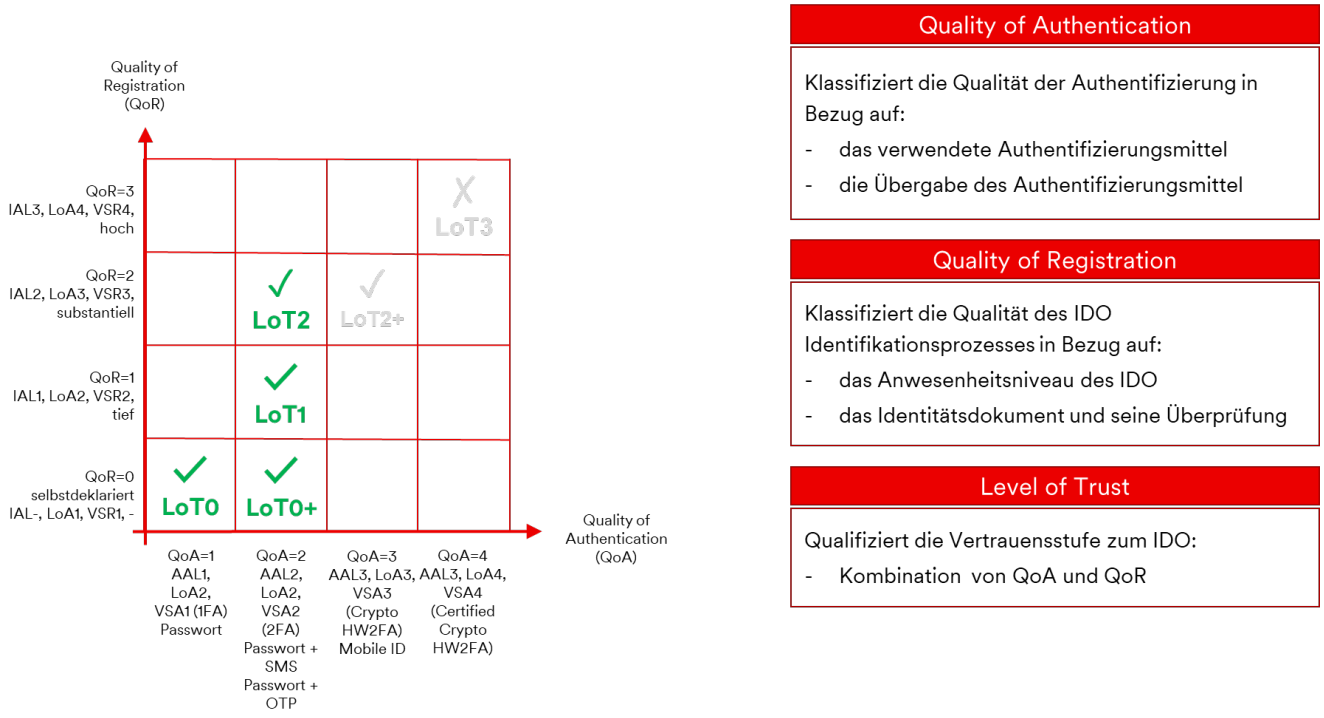


Abbildung 4: Die unterschiedlichen Vertrauensstufen der SwissID

#### 3.1.1 Qualität der Authentifizierung (QoA)

Die Qualität der Authentifizierung wird durch die Anzahl und Art der Authentifizierungsfaktoren definiert, die beim Login mit SwissID zur Anwendung kommen. Die tiefste Stufe der Authentifizierung stellt dabei die Ein-Faktor-Authentifizierung dar (Passwort). Die Zwei-Faktor-Authentifizierung ist eine Kombination von mehreren unabhängigen Faktoren und erfüllt damit höhere Sicherheitsansprüche. Beim Login mit SwissID bieten sich folgende Methoden an: Login über eine Kombination von Passwort und SwissID-App, Mobile ID oder SMS-Code. Die «Qualität der Authentifizierung», die zur Identifikation des SwissID Inhabers bei einem Onlinedienst dient, wird durch den Onlinedienstanbieter definiert.

| Implementation | NIST | ISO | eCH-0170 | eIDAS / BGEID | SwissID QoA |
|---|---|---|---|---|---|
| Passwort | AAL1 | LoA2 | VSA1 | niedrig | QoA 1 |
| SMS | AAL1 | LoA2 | VSA1 | niedrig | QoA 1 |
| Streichliste | AAL1 | LoA2 | VSA1 | niedrig | QoA 1 |
| Passwort + SMS | AAL2 | LoA2 | VSA2 | niedrig | QoA 2 |
| Passwort + Streichliste | AAL2 | LoA3 | VSA2 | niedrig | QoA 2 |
| Mobile ID | AAL3 | LoA3 | VSA3 | substanziell | QoA 3 |
| SwissID App | AAL3 | LoA3 | VSA3 | substanziell | QoA 3 |
| Crypto Token | AAL3 | LoA4 | VSA4 | hoch | QoA4 |

*Abbildung 5: Die Authentifizierungsmittel von SwissID*

### *3.1.2* Qualität der Registrierung (QoR):

Die Qualität der Registrierung definiert sich durch die Art und Weise, wie die Identität des SwissID Inhabers sowie die Qualität des dazu verwendeten Authentifizierungsmittels überprüft wird.

| Quality of registration | NIST | ISO | eCH-0170 | eIDAS / BGEID | SwissID QoR |
|---|---|---|---|---|---|
| Anlegen einer neuen SwissID | IAL1 | LoA1 | VSR1 | - | QoR 0 |
| Photo Identifikationsprozess | IAL1 | LoA2 | VSR2 | niedrig | QoR 1 |
| Import SuisseID/Gelbe ID ID@Office mit Prüfung des ID Dokuments | IAL2 | LoA3 | VSR3 | substanziell | QoR 2 |
| ID@PostOffice mit Prüfung des ID Dokuments | IAL2 | LoA3 | VSR3 | substanziell | QoR2 |
| RA App | IAL2 | LoA3 | VSR3 | substanziell | QoR2 |

**Bemerkung:** Die Angaben zur E-ID stellen die aktuelle Interpretation des in der Botschaft zur E-ID verwendeten Gesetzestextes dar. Änderungen bleiben vorbehalten.

*Abbildung 6: Die verschiedenen Qualitätsstufen der Identifikation SwissID*

### 3.2 Austausch von Attributen: Die Funktion «Informationen freigeben»

Bei der Abwicklung von Onlinegeschäften spielt das Teilen von Attributen zwischen dem SwissID Inhaber und dem Onlinedienstanbieter die wichtigste Rolle.

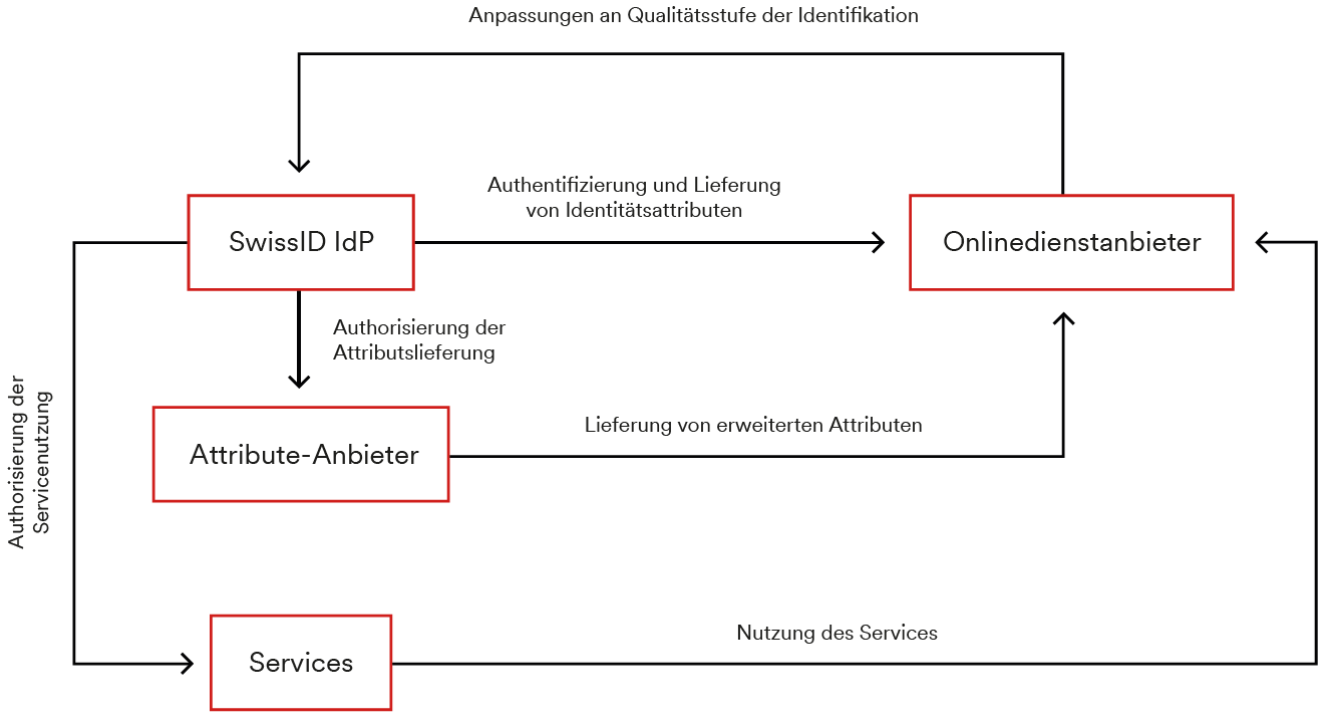


*Abbildung 7: Darstellung der technischen Schnittstellen zwischen den Teilnehmern des SwissID Ökosystems*

Die Authentifikation und das Vermitteln der (Identitäts-)Attribute wird über den IdP abgewickelt.

Dabei steht der Datenschutz an oberster Stelle. Dieser wird durch die folgenden Grundsätze sichergestellt:

- Der SwissID Inhaber hat jederzeit die Kontrolle und Hoheit darüber, welche Identitätsattribute welchem Onlinedienstanbieter zur Verfügung gestellt werden. Identitätsattribute werden dem Onlinedienstanbieter nur für den notwendigen Geschäftsvorfall und nach der Freigabe des SwissID Inhabers bekanntgegeben. Der SwissID Inhaber kann die Freigaben jederzeit zurückziehen.
- Es gilt immer der Grundsatz der Datensparsamkeit, d.h. dass nur diejenigen Attribute durch den Onlinedienstanbieter bezogen werden, die für den entsprechenden Geschäftsvorfall notwendig sind. Das bedeutet, dass sich der SwissID Inhaber dank SwissID «anonym» auf einer Plattform bewegen und sich im gleichen Zuge sich gegenüber dem Onlinedienstanbieter ausweisen kann – immer unter Wahrung der Datenkontrolle/-hoheit.
- SwissID verarbeitet und analysiert zu keiner Zeit Informationen darüber, bei welchem Onlinedienstanbieter und zu welchem Zweck sich ein SwissID Inhaber einloggt. Die Daten werden weder verkauft noch für kommerzielle Zwecke an Dritte weitergegeben.

## 4 Sicherheitsrelevante Leitlinien für das Ökosystem von SwissID

Das Leistungsangebot des IdP zielt darauf ab, die digitalen Geschäftsprozesse möglichst einfach zu gestalten. Hoch vertrauenswürdige Kommunikations- und Transaktionsflüsse sollen unterstützt werden, ohne dass dadurch die Komplexität zunimmt. SwissID als vertrauenswürdige Identität ist dabei ein zentraler Baustein im Angebot der SwissSign Group AG. SwissSign Group AG wird auch als IdP im Sinne des E-ID-Gesetzes die entsprechende Anerkennung anstreben. SwissSign ist heute schon ein anerkannter Trust Service Provider (TSP) und erfüllt die Anforderungen der ZertES.

Entsprechend hoch ist der Stellenwert der Sicherheit bei der SwissSign Group AG – in der Geschäftsstrategie, in der betrieblichen Architektur, der Führung und auch in der Firmenkultur.

Das strategische Programm des IdP – das Cybersecurity Maturity Improvement Program – ist der kontinuierlichen Verbesserung im Bereich Cybersecurity gewidmet. Das Programm orientiert sich dabei an einem Maturitätsmodell aus der Familie der Capability Maturity Model Integration (CMMI).

Diese Maturitäts- oder Reifegradmodelle beinhalten jeweils eine systematische Aufbereitung bewährter Standards/Praktiken, um die Verbesserung einer Organisation zu unterstützen. Während eine Zertifizierung gemäss einem Sicherheitsstandard, das Vorhandensein bestimmter Prüfpunkte belegt, zielt der beim IdP verwendete CMMI-Cybermaturity-Ansatz auf die nachhaltige Verankerung von Sicherheit in der Organisation ab. Damit wird dann auch die nachhaltige Verankerung der Prüfpunkte garantiert.

Der CMMI-Cybermaturity-Ansatz konsolidiert die Konzepte und Praktiken der bestimmenden Standards im Bereich Cybersecurity:

- NIST Framework for Improving Critical Infrastructure Cybersecurity
- ISO/IEC 27001: Information technology – Security techniques – Information Security Management Systems – Requirements
- ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security controls
- NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations
- CIS Top 20 Critical Security Controls
- COBIT 5: A Business Framework for the Governance and Management of Enterprise IT
- CMMI Threat Kill Cycle (TKC)

Eine regelmässige Aktualisierung (zweimal im Jahr) garantiert dabei, dass der CMMI-Cybermaturity-Ansatz immer die neusten Erkenntnisse bezüglich Cybersecurity reflektiert.

Das Sicherheitsdenken beim IdP ist ganzheitlich angelegt und adressiert mit seinen Massnahmen alle Dimensionen der Geschäftsarchitektur – Strategie, Mitarbeitende, Prozesse und Technologie. Die strategische Ausrichtung des Cybersecurity Maturity Improvement Programms wird auf Basis eines aus der Geschäftsstrategie abgeleiteten gemeinschaftlichen Verständnisses der ICT «Kronjuwelen» sowie einer Beurteilung der Gesamtlage bezüglich aktueller Cyber-Risiken wird auf Ebene der Geschäftsleitung definiert. Daraus ergeben sich die Prioritäten für die kontinuierlichen Verbesserungsmassnahmen in den weiteren Dimensionen.

Nebst fortlaufenden Verbesserungen in Prozessen und der Technologie ist die Verankerung des Sicherheitsdenken in der Unternehmenskultur ein weiteres zentrales Anliegen dieses Programms. Eine kontinuierliche Cyber-Security-Awareness-Kampagne zielt darauf ab, das Bewusstsein der Mitarbeitenden bezüglich Cyber-Risiken zu schärfen – das Fundament für eine nachhaltige und ganzheitliche Sicherheit.

# 5 Entwicklung

Im Entwicklungsprozess liegt der Fokus auf der Sicherheit und Qualität der Software, um damit Probleme zu minimieren, die aus potenziellen Softwarefehlern entstehen. Die Software muss bei der Integration in das produktive System mehrere Qualitätssicherungstests in verschiedenen Umgebungen durchlaufen.

## 5.1 Produktlebenszyklus

Ergänzend zum CMMI-Cybermaturity-Ansatz orientiert sich der IdP hier am Software Assurance Maturity Model (SAMM). Dieses Modell definiert vier kritische Geschäftsfunktionen – Führung, Entwicklung, Verifizierung und Betrieb – mit denen der ganze Product-Management-Lifecycle und dessen Steuerung abgedeckt ist.

### Führung

Die übergreifende strategische Ausrichtung des SAMM Programms und die Instrumentierung von Prozessen und Aktivitäten ergeben Kennzahlen, welche die Sicherheitslage des Unternehmens aufzeigen. Anhand dieser internen Kennzahlen wird die Sicherheitslage transparent gemacht und Gegenmassnahmen können frühzeitig eingeleitet werden.

Die internen Sicherheits-, Compliance-, Kontroll- und Audit-Mechanismen der Organisation, insbesondere der Entwicklungsteams, ermöglichen eine erhöhte Sicherheit in der sich im Aufbau und im Betrieb befindlichen Software.

Stete Ausbildung und gegenseitiger Austausch der Mitarbeitenden beinhaltet die Erweiterung des Sicherheitswissens in der Softwareentwicklung z.B. durch Schulungen und Beratung zu Sicherheitsthemen, die für die einzelnen Berufsfunktionen relevant sind.

### Entwicklung

Die Bedrohungsanalyse beinhaltet die genaue Identifizierung und Charakterisierung potenzieller Angriffe auf die Software eines Unternehmens, um die Risiken besser zu verstehen und das Risikomanagement zu erleichtern.

Der Einbezug von Sicherheitsanforderungen in den Softwareentwicklungsprozess legt den Grundstein, damit sicherheitsrelevante Aspekte in der Software von Anfang an berücksichtigt werden.

Sichere Architektur bringt die Unterstützung des Designprozesses zur Förderung sicherer Standarddesigns und der Kontrolle über Technologien und Frameworks, auf denen die Software basiert.

### Verifizierung

Mithilfe fachlicher Reviews werden die nächsten Entwicklungsschritte bereits vor der Umsetzung verifiziert und auf ihre Sicherheit und die Vollständigkeit geprüft.

Das Design Review beinhaltet die Überprüfung der aus dem Designprozess entstandenen Artefakte, um sicherzustellen, dass adäquate Mechanismen zur Verfügung stehen und die Sicherheitserwartungen einer Organisation eingehalten werden.

Das Code Review beinhaltet die Bewertung des Quellcodes einer Organisation, um die Verwundbarkeit und die damit verbundenen Schadensminderungsaktivitäten zu unterstützen und eine Grundlage für sichere Codierungserwartungen zu schaffen.

Durch Security Testing wird die Software in seiner Laufzeitumgebung getestet, um sowohl Schwachstellen zu erkennen als auch einen Mindeststandard für Software-Releases festzulegen. In diesem Prozess sind ebenfalls extern organisierte Penetrationstests enthalten.

Durch funktionales Testing werden die in den Anforderungen spezifizierten Resultate geprüft.

Mithilfe von Regressionstests wird die Funktionalität der bestehenden Software in der Qualität gesichert. Die Regressionstestsets werden mit jedem Release durch die neuen Testfälle erweitert.

Durch automatisiertes Testing werden regelmässige Qualitätssicherungen vorgenommen, um die kontinuierliche Qualität sicherzustellen.

### Betrieb

Das Management der Angreifbarkeit etabliert konsistente Prozesse für interne und externe Reports über die Verwundbarkeit des Systems, um die Exponierung der Software zu begrenzen und Daten zu sammeln, damit die Sicherheitsgewährleistung verbessert werden kann.

Härtung beinhaltet die Implementierung von Kontrollen für die Betriebsumgebung um die Software eines Unternehmens und die Sicherheitslage der eingesetzten Anwendungen zu verbessern.

Die Sicherstellung der Betriebsbereitschaft beinhaltet die Identifizierung und Erfassung sicherheitsrelevanter Informationen, die ein Operator benötigt, um die Software einer Organisation richtig zu konfigurieren, einzusetzen und auszuführen.

## 5.2 Entwicklungsmethodik

In der Entwicklung selbst richtet sich der IdP nach der Security-Aware-Development-Methode, die spezifisch auf die Herausforderungen einer agilen Entwicklung ausgestaltet ist.

Der eingesetzte Entwicklungsprozess stellt sicher, dass IT-Sicherheitsanforderungen von Anfang an mitberücksichtigt werden und die IT-Sicherheit im Zentrum der Entwicklungstätigkeit steht.

# 6 Data Governance und Datenschutz

## 6.1 Rechtsbeziehungen im SwissID Ökosystem

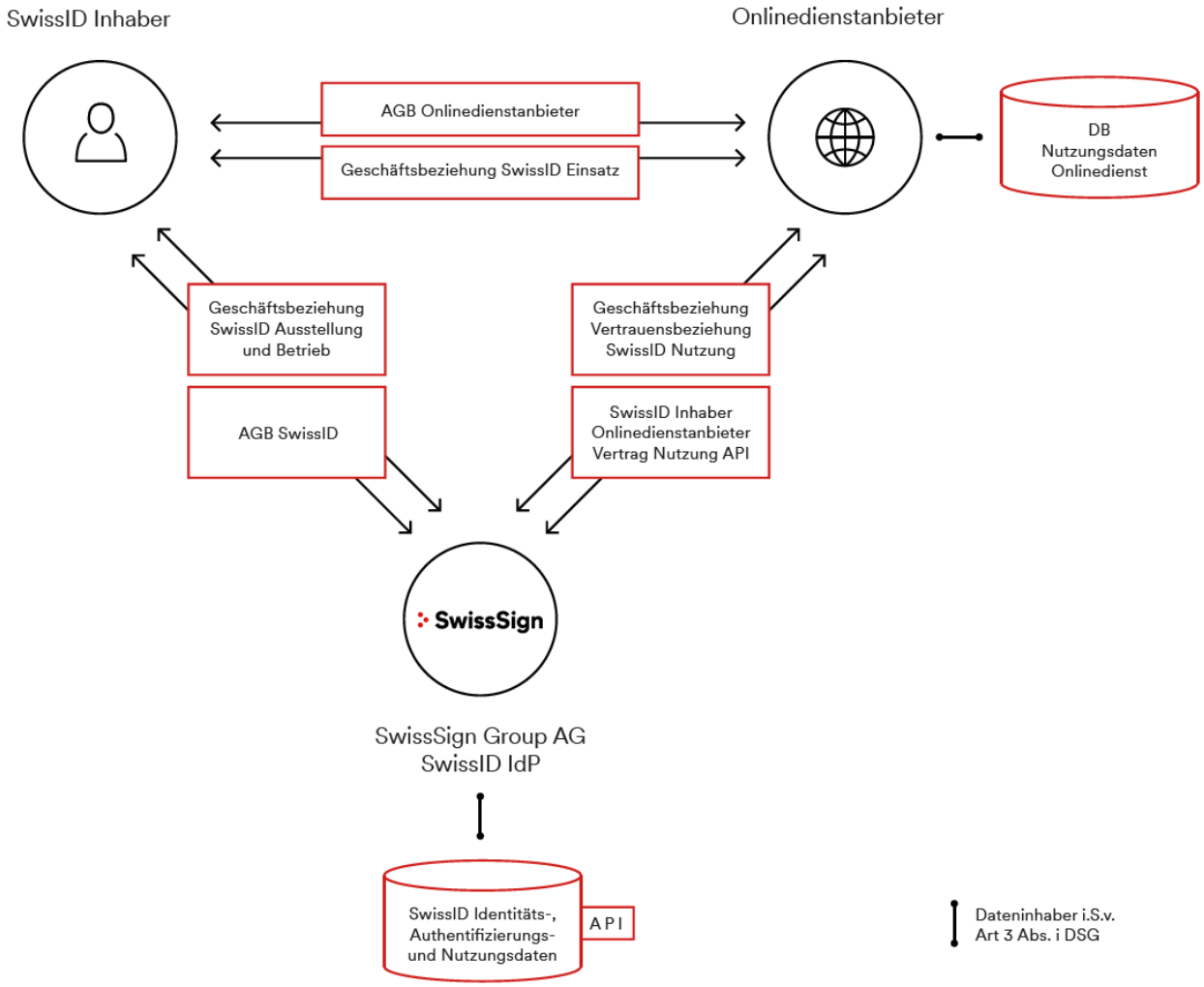


Abbildung 8: Rechtsbeziehungen im Ökosystem von SwissID: Verhältnis IdP – SwissID Inhaber

Jeder SwissID Inhaber schliesst mit der SwissSign Group AG (IdP) einen Vertrag ab. Diese Rechtsbeziehung wird durch die AGB von SwissID für den SwissID Inhaber abschliessend geregelt. In den AGB ist definiert, dass der IdP die Übermittlung der Identitätsdaten eines SwissID Inhabers an den Onlinedienstanbieter ausschliesslich mit Einwilligung des SwissID Inhabers vornimmt und damit die volle Verantwortung für die datenschutzkonforme Bearbeitung der Daten trägt. Die im Zusammenhang mit der Nutzung von SwissID bearbeiteten Daten werden dem IdP ausschliesslich vom SwissID Inhaber oder von Dritten zum nachgenannten Zweck bekanntgegeben. Die Bekanntgabe und Erfassung der Daten erfolgt im Rahmen der Registrierung sowie der Nutzung von SwissID durch den SwissID Inhaber.

### 6.2 Verhältnis IdP –Onlinedienstanbieter

Das Verhältnis „IdP – Onlinedienstanbieter“ betreffend SwissID ist im **Vertrag mit dem Onlinedienstanbieter** geregelt. Der Onlinedienstanbieter erhält ein vertraglich differenziert geregeltes Recht zur Nutzung eines API zu den SwissID Systemen zwecks Bezugs der von SwissID Inhabern freigegebenen Daten. Der IdP bearbeitet keine Daten im Auftrag des Onlinedienstanbieters. Die Entscheidungshoheit über Daten (Identitäts-, Authentifikations- und Nutzungsdaten) liegt einzig beim IdP. Die Daten werden gemäss den Vereinbarungen mit den SwissID Inhabern an die Onlinedienstanbieter übermittelt.

Für die Nutzung der API gelten folgende Regeln:

- **Kontrolle des SwissID Inhabers:** Attributsdaten eines SwissID Inhabers werden dem Onlinedienstanbieter nur bei einer bewussten Freigabe des SwissID Inhabers übermittelt, z.B. indem er sich mittels SwissID beim Onlinedienst einloggt und die Übermittlung von seinen Daten freigibt. Der Onlinedienstanbieter erhält im Ergebnis nur die Attributsdaten über seine eigenen Kunden (SwissID Inhaber). Über den Consent Screen kann der SwissID Inhaber bewusst bestimmen, welche Attributsdaten er an den Onlinedienstanbieter übermittelt.
- **Read only:** Es findet kein Datenfluss vom Onlinedienstanbieter zum SwissID-Konto des SwissID Inhabers statt.
- **Unabhängigkeit:** Der IdP macht dem Onlinedienstanbieter keine Vorgaben betreffend die Regelung des Verhältnisses „Onlinedienstanbieter – SwissID Inhaber“. Der Onlinedienstanbieter soll die SwissID Inhaber zur Sorgfalt im Umgang mit den Authentifizierungsdaten verpflichten.
- Das SwissID-System legt für jeden SwissID Inhaber eine **technische Kennung (die sogenannte UUID) für jeden Onlinedienst** fest. Mittels dieser jeweils unterschiedlichen UUID kann der SwissID Inhaber nicht über mehrere Onlinedienste hinweg identifiziert werden.
- Der Onlinedienstanbieter wird darauf hingewiesen, dass einzelne Attribute **besonders schützenswerte Personendaten** enthalten (z.B. Gesichtsbild in Ausweiskopie).
- **Eigenverantwortung Onlinedienstanbieter:** Der Onlinedienstanbieter gibt die Daten eines SwissID Inhabers gemäss der Vereinbarung bekannt, die der SwissID Inhaber als Kunde mit dem Onlinedienstanbieter hat. Im Rahmen dieser Vereinbarungen und der gesetzlichen Datenschutzordnung kann SwissID dem Onlinedienstanbieter diese sowie andere über den Kunden erfasste Daten (Kundendaten[2]) bearbeiten. Der Onlinedienstanbieter trägt für diese Daten eigenständig die volle datenschutzrechtliche Verantwortung gegenüber ihren Kunden.
- Dank SwissID muss der Onlinedienstanbieter keine Authentifizierungsmerkmale seiner Kunden mehr erfassen. Er kann sich auf die im Rahmen der Registrierung erfassten Attribute verlassen. Der Onlinedienstanbieter muss die mit der SwissID seiner Kunden verbundenen Basisdaten (z.B. echtheitsbestätigte Ausweiskopie) nicht beziehen, sondern erhält eine Bestätigung, dass diese bei der IdP vorhanden sind. Nur wenn der Onlinedienstanbieter zur Dokumentation gesetzlich verpflichtet ist (z.B. GwG, ZertES), können z.B. Ausweiskopien an Der Onlinedienstanbieter übermittelt werden.

[2] Anwenderdaten: Die Gesamtheit der beim Onlinedienstanbieter bearbeiteten Kundendaten

## 6.3 Regeln und Prinzipien des Datenschutzes von SwissID

### Datentypen und Speicherung

Die SwissID-Daten werden nach Umgang, Lebenszyklus, Persistenz und Archivierung unterschieden und folgenden Kategorien zugeteilt:

- **Identitätsdaten** (mit Personenbezug): Angaben über den SwissID Inhaber, entweder selbstdeklariert oder geprüft. Damit der SwissID Inhaber auch qualifiziert signieren kann, unterstehen diese Daten auch dem ZertES.
- **Authentifizierungsdaten** (mit Personenbezug): Credentials, 2FA-Einstellungen werden gemäss aktuellem Entwicklungsstand der Technik zwischengespeichert (verschlüsselt), jedoch nicht aufbewahrt.
- **Nutzungsdaten** (mit Personenbezug): Freigaben und Nutzung (z.B. wann und wo hat sich der Anwender mit welcher IP-Adresse angemeldet, Anzahl fehlgeschlagener Loginversuche). Damit der SwissID Inhaber auch qualifiziert signieren kann, unterstehen diese Daten auch dem ZertES (Nachvollziehbarkeit, Aufbewahrungsfristen). Die erhobenen Daten werden NICHT für das Erstellen von Anwender-Konten verwendet.
- **Systemdaten** (ohne Personenbezug): Log-, Konfigurations- und Auditdaten. Diese Daten dienen dem Zweck, den Zustand des Systems zu überwachen und werden spätestens nach einem Jahr vernichtet.

### Zweck der Nutzung

Die Daten eines SwissID Inhabers werden ausschliesslich im Zusammenhang mit der Nutzung von SwissID genutzt. Der IdP (SwissSign Group AG) verwendet die Daten niemals für das Erstellen von Persönlichkeitsprofilen.

Mit SwissID stellt der IdP natürlichen Personen eine digitale Identität (SwissID) zur Authentifikation im Internet gegenüber Onlinedienstanbietern zur Verfügung. Die digitale Identität besteht aus verschiedenen Authentifizierungskomponenten sowie zusätzlichen Angaben des Kunden. Im Rahmen des Einsatzes von SwissID kann der SwissID Inhaber seine Identitätsdaten an den Onlinedienstanbieter übermitteln.

### Transparenter und sicherer Umgang mit den Daten des SwissID Inhabers

Die Anwenderdaten zwischen dem IdP und dem Onlinedienstanbieter werden nur mit Einwilligung des SwissID Inhabers (Opt-in) ausgetauscht (Privacy by Default). Der SwissID Inhaber muss jeder Datenübergabe zustimmen. Dazu hat er die Möglichkeit, einen «persistent consent» für sämtliche Onlinedienstanbieter abzugeben, ohne eine Zustimmung für jede einzelne Datenübergabe abzufragen.

Der SwissID Inhaber hat die Hoheit über seine Daten und steuert an, welchem Onlinedienstanbieter er welche Daten freigibt. Die Freigaben kann er in seinem SwissID-Konto auf swissid.ch einsehen und auch jederzeit zurückziehen.

### Schutz der Daten der SwissID Inhaber durch Technikgestaltung (Privacy by Design)

Jeder SwissID Inhaber erhält für jeden genutzten Onlinedienst eine einzigartige technische Kennung - die sogenannte UUID. Daraus abgeleitet gilt:

- Eine technische Zusammenführung der Anwenderdaten über mehrere Onlinedienstanbieter hinweg ist auf Basis unterschiedlicher UUIDs nicht möglich (Privacy by Design).
- Der SwissID Inhaber präsentiert sich bei jedem Onlinedienstanbieter immer mit der gleichen eineindeutigen technischen Kennung.
- Die technische Kennung des SwissID Inhabers bei den verschiedenen Onlinedienstanbieter kennt einzig der IdP. Hierbei wird keine Datentabelle (Datenbank) verwendet, sondern ein nur dem IdP zugänglicher Algorithmus.

Im Weiteren gilt es zu beachten, dass die SwissSign Group AG die Identitätsattribute des SwissID Inhabers immer getrennt von den Nutzungsdaten aufbewahrt.

### Datenhaltung in der Schweiz

Die Datenhaltung im Kontext von SwissID durch den IdP erfolgt ausschliesslich in sicheren Rechenzentren in der Schweiz. Die Rechenzentren erfüllen nebst anderen hohen Anforderungen auch denjenigen des Rundschreibens 2018/3 „Outsourcing – Banken und Versicherer".

## 7 Technische und organisatorische Massnahmen zur Datensicherheit

### 7.1 Zugangskontrolle (Art.9 lit. a VDSG)

Ziel der Zugangskontrolle (Zutrittskontrolle) ist es, Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden.

**Massnahmen:**

Die SwissID Server stehen in geschützten Rechenzentren (RZ), welche über ein mehrstufiges Sicherheitskonzept verfügen und nach dem Raum-im-Raum-Prinzip gebaut sind.

Zu den Sicherheitsmerkmalen gehören:

- Die RZ-Gebäude sind an spezifischen Stellen videoüberwacht. Die Haupteingänge werden aus dem Innenbereich überwacht.
- Sicherheitsrelevante Eingänge sind alarmgesichert.
- Ohne Identitätsnachweis kann niemand das Gebäude betreten, alle Besucher werden mit einer kundenspezifischen Berechtigungsliste abgeglichen und begleitet.
- Die RZ-Bereiche sind umfassend mit Schlüsselkarten (Badge) und biometrischen Lesern ausgerüstet.

### 7.2 Personendatenträgerkontrolle (Art.9 lit. b VDSG)

Ziel der Personendatenträgerkontrolle ist es, unbefugten Personen das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verunmöglichen.

**Massnahmen im Bereich Zutritte:**

- Alle Zutritte zu den Gebäuden werden durch Zutrittskontrollen gesichert.
- Alle Zutritte müssen über einen Standardprozess beantragt werden.
- Der Zutritt wird über kontaktlose Schlüsselkarten (Badge) erteilt.
- Bei Aus-/ Übertritt werden die Berechtigungen gemäss dem Standardprozess entzogen.
- Die Zutritte werden periodisch überprüft.

**Massnahmen im Bereich Zugriffe:**

- Berechtigungen werden einem eindeutigen und grundsätzlich persönlichen Benutzerkonto zugewiesen.
- Die Bündelung von Berechtigungen erfolgt grundsätzlich rollenbasiert auf Basis des zentralen Identity Management-Systems (IDM) und nach dem «Need-to-know-Prinzip».
- Alle Zugriffe auf Daten müssen im Identity- und Access Management-System (IAM) beim Dateneigner beantragt werden.
- Risikobasiert wird auch eine Zwei-Faktor-Authentifizierung eingesetzt.
- Der Dateneigner wird periodisch zur Überprüfung aufgefordert.
- Bei Aus- / Übertritt werden die Berechtigungen gemäss standardisierten IAM-Prozessen entzogen (Account gesperrt).

### 7.3 Transportkontrolle (Art.9 lit. c VDSG)

Ziel der Transportkontrolle (Weitergabekontrolle) ist es zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung, während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

**Massnahmen:**

- Die **Übergabe der Daten an den Onlinedienstanbieter findet verschlüsselt** statt. Dabei kommen die aktuellen TLS-Protokolle zum Einsatz, um den Onlinedienst zu identifizieren und authentifizieren.

### 7.4 Bekanntgabekontrolle (Art.9 lit. d VDSG)

Ziel der Bekanntgabekontrolle ist es, dass Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, identifiziert werden können.

**Massnahmen:**

- Alle Onlinedienstanbieter, die an den IdP angebunden sind, benötigen einen Vertrag und werden bei jeder Anfrage am IdP authentifiziert.
- Zusätzlich muss der SwissID Inhaber über einen Consent-Screen seine Einwilligung zur Bekanntgabe geben.
- Ausser auf richterliche Anweisung werden an andere Dritte keine Personendaten übergeben.

### 7.5 Speicherkontrolle (Art.9 lit. e VDSG)

Ziel der Speicherkontrolle ist es, unbefugte Eingabe in den Speicher sowie unbefugte Einsichtnahmen, Veränderungen oder eine Löschung gespeicherter Personendaten zu verhindern.

**Massnahmen:**

- Es besteht ein zentrales Identity- und Access Management-System (IAM) mit standardisiertem Bewilligungsprozess.
- Alle Zugriffe auf Daten müssen im IAM beim Dateneigner beantragt werden.
- Die Zugriffe werden mittels Gruppen / Rollen vergeben.
- Risikobasiert wird auch eine Zwei-Faktor-Authentifizierung eingesetzt.
- Der Dateneigner wird periodisch zur Überprüfung aufgefordert.
- Bei Aus- / Übertritt werden die Berechtigungen gemäss standardisierten IAM Prozessen entzogen (Account gesperrt).

### 7.6 Benutzerkontrolle (Art.9 lit. f VDSG)

Ziel der Benutzerkontrolle (Zugangskontrolle) ist es, mithilfe geeigneter Massnahmen zu verhindern, dass Unbefugte Datenverarbeitungssysteme, mit denen personenbezogener Daten verarbeitet oder genutzt werden, nutzen können, sowie die Benutzung von automatisierten Datenverarbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen zu verhindern.

**Massnahmen:**

- Administrative Zugriffe erfolgen ausschliesslich über die dafür vorgesehene Admin-Zone unter Verwendung einer starken Authentifikation und ausschliesslich verschlüsselt.
- Der Zugriff in die Admin-Zone erfolgt authentisiert mittels user- und/oder applikationsbasierenden Firewall-Regeln.
- Direkte Verbindungen von Access-Zone in die Admin -Zone sind untersagt.
- Dritte / Partner haben keinen Zugriff in die Admin-Zone.
- Das Systemmanagement aller Netzwerkkomponenten und Systeme erfolgt ausschliesslich ausgehend von den internen Kommunikationsnetzen mit dem Trust Level «trusted».
- Die Nachvollziehbarkeit wird bedarfsgerecht gewährleistet, (alle administrativen Aktivitäten, erfolgreiche und nicht erfolgreiche Anmeldeversuche etc.).

### 7.7 Zugriffskontrolle (Art.9 lit. g VDSG)

Ziel der Zugriffskontrolle ist es, den Zugriff der berechtigten Personen auf diejenigen Personendaten zu beschränken, die sie für die Erfüllung ihrer Aufgabe benötigen.

**Massnahmen:**

- Die Zugriffsrechte auf die entsprechenden Systeme werden über Rollen (Systemadministrator, Applikationsverantwortlicher, Support-Mitarbeiter) definiert.
- Die Zugriffe werden auf den jeweiligen Systemen und Applikationen protokolliert. Diese Protokolle werden gemäss Geschäftsbücherverordnung archiviert.
- Es besteht ein zentrales Identity- und Access Management-System (IAM) mit standardisiertem Bewilligungsprozess.
- Berechtigungen werden einem eindeutigen und grundsätzlich persönlichen Benutzerkonto zugewiesen.
- Die Bündelung von Berechtigungen erfolgt grundsätzlich rollenbasiert auf Basis des zentralen IDM und nach dem «Need-to-know-Prinzip».
- Betriebs- und sicherheitsrelevante Ereignisse werden bedarfsgerecht aufgezeichnet und überwacht.
- Protokollierungsinformationen sind vor Verfälschung und unbefugtem Zugriff geschützt und werden über den geforderten Zeitraum aufbewahrt.

### 7.8 Eingabekontrolle (Art.9 lit. h VDSG)

Ziel der Eingabekontrolle ist es, dass nachträglich festgestellt werden kann, ob und von wem personenbezogene Daten in die Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

**Massnahmen:**

- Jeder Teilnehmer an der SwissID IdP-Plattform ist identifiziert und authentifiziert. Die entsprechenden Tätigkeiten werden protokolliert.
- Die Tätigkeiten der Operatoren der SwissID-IdP-Plattform werden protokolliert.
- Berechtigungen werden einem eindeutigen, persönlichen Benutzerkonto zugewiesen, ausgenommen davon sind beispielsweise Backup, Monitoring und applikatorische Datenbankzugriffe.
- Die Bündelung von Berechtigungen erfolgt rollenbasiert auf Basis des zentralen IDM und nach dem «Need-to–know-Prinzip».
- Die SwissID Betreiberin verfügt über ein zentrales IAM mit standardisiertem Bewilligungsprozess
- Betriebs- und sicherheitsrelevante Ereignisse werden bedarfsgerecht aufgezeichnet und überwacht.
- Protokollierungsinformationen sind vor Verfälschung und unbefugtem Zugriff geschützt und werden über den geforderten Zeitraum aufbewahrt.

### 7.9 Verfügbarkeitskontrolle

Ziel der Verfügbarkeitskontrolle ist es, zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

**Massnahmen:**

- Die Infrastruktur ist redundant aufgebaut und die Account- und Transaktionslogdaten werden gesichert (Backup).
- Angemessene Massnahmen zum Schutz gegen Malware werden getroffen. Ergänzend werden Verfahren umgesetzt, um einen möglichen Befall frühzeitig zu erkennen und den ordnungsgemässen Betrieb sicherzustellen.
- Erkannte Schwachstellen werden methodisch bewertet und entsprechende Massnahmen risikogerecht festgelegt.
- Es bestehen geeignete Verfahren für eine anforderungsgerechte Datensicherung und Wiederherstellung. Die Verfahren werden periodisch getestet.
- Vorgaben zur Sicherstellung des Geschäftsbetriebs (Business Continuity / IT Service Continuity Management) sind definiert und entsprechende Prozesse und Verfahren umgesetzt.
- Auf Basis der individuellen Geschäftsanforderungen bestehen konkrete Wiederanlaufpläne und -klassen. Die Wiederanlaufverfahren sind standardisiert und an zentraler Stelle dokumentiert

- Durch periodische Tests und Neubeurteilung der Wiederanlaufverfahren ist gewährleistet, dass die Dokumentationen aktuell und funktionsfähig bleiben.

### 7.10 Trennungskontrolle

Ziel der Trennungskontrolle ist es, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Zweckbindung).

**Massnahmen:**

- SwissID-Applikationen laufen auf dedizierten Servern und in dedizierten Netzwerkzonen (logische Trennung der Kommunikationsnetze).
- Systeme für Test und Entwicklung werden grundsätzlich auf einer von der Produktion und Integration separierten Plattform betrieben.
- Die Kommunikation zwischen Areas ist durch Security Devices (z.B. Firewalls) eingeschränkt.
- Systeme werden nach definierten Kriterien in den Netzwerkzonen platziert.

**Literaturquellen:**

| Dokument | Quelle: |
|---|---|
| eCH-170 VSR1 – VSR4 | https://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0170 |
| DSG | https://www.admin.ch/opc/de/classified-compilation/19920153/index.html |
| FINMA Rundschreiben 2008/7 zum Outsourcing der Banken | https://www.finma.ch/de/~/.../finma/.../myfinma/rundschreiben/finma-rs-2008-07.pdf |
| NIST None – IAL 3 | https://pages.nist.gov/800-63-3/sp800-63a/sec1_2_introduction.html |
| VDSG | https://www.admin.ch/opc/de/classified-compilation/19930159/201210160000/235.11.pdf |