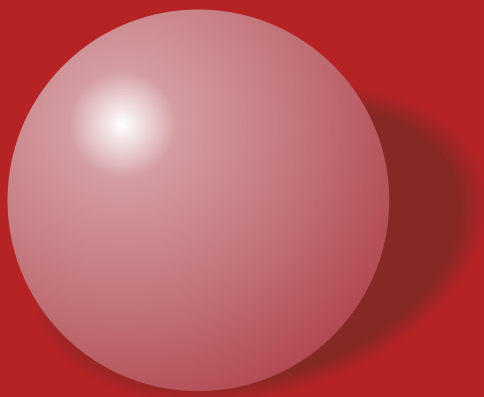
Michael Quade | Ralf Wölfle

SuisseID in der Praxis

Grundlagen und Fallstudien zum elektronischen Identitätsnachweis der Schweiz



eXperience

Michael Quade | Ralf Wölfle

SuisseID in der Praxis

Grundlagen und Fallstudien
zum elektronischen Identitätsnachweis
der Schweiz

edition esowip

Inhalt

Was ist die SuisseID?

Die SuisseID ist das standardisierte Schweizer System, mit dem über elektronische Dienste wie das Internet Personen eindeutig identifiziert und Geschäfte rechtsgültig abgeschlossen werden können. Das System besteht aus mehreren Hard- und Softwarekomponenten sowie aus definierten Regeln und Verfahren, die zusammen das gewünschte hohe Sicherheitsniveau erzielen.

Der Anwender kommt mit der SuisseID über das SuisseID-Token in Kontakt. Das Token ist die Hardwarekomponente auf der Client-Seite. Sie hat das Erscheinungsbild einer Smartcard mit integriertem Chip, ähnlich einer Kreditkarte oder einer SIM-Karte, wie sie auch in Mobiltelefonen eingesetzt wird. Die SuisseID auf einer SIM-Karte wird in einen USB-Stick eingesetzt und über diesen an den Computer des Benutzers angeschlossen. Bei Smartcards wird ein geeignetes Lesegerät benötigt, das in modernen Notebooks häufig eingebaut ist.

Wird die SuisseID an einen Computer angeschlossen, kann sie für den elektronischen Identitätsnachweis (Authentifizierung) und für die elektronische Unterschrift (Signatur) verwendet werden. Für Freigabe dieser Funktionen muss eine persönliche Identifikationsnummer (PIN) eingegeben werden:

- Elektronischer Identitätsnachweis (Authentifizierung): Die SuisseID erlaubt, elektronische Dienste in Anspruch zu nehmen, die eine sichere Identifizierung voraussetzen. Die Identifizierung mit der SuisseID ist vergleichbar mit dem Vorweisen einer Identitätskarte oder eines Passes. Ein Inhaber kann mit der SuisseID elektronisch beweisen, wer er ist.
- Qualifizierte elektronische Unterschrift (Signatur): Mit der SuisseID können elektronische Dokumente rechtsgültig unterschrieben werden. Die qualifizierte elektronische Signatur ist per Gesetz der eigenhändigen Unterschrift gleichgestellt.

Die SuisseID wird in den folgenden Kapiteln nach und nach erklärt. Nach der Vorstellung der gesetzlichen Rahmenbedingungen wird erläutert, inwiefern die SuisseID ein Standard ist. Es folgt eine detaillierte Vorstellung der Funktionen der SuisseID, wobei sowohl die Abläufe als auch die dabei genutzte Infrastruktur dargestellt werden.

Gesetzliche Rahmenbedingungen

Damit die Rechtssicherheit der qualifizierten elektronischen Unterschrift mit der SuisseID gewährleistet ist, wurden in der Schweiz in den letzten Jahren mehrere Gesetze und Verordnungen erlassen oder geändert.

Die Rechtsgrundlage für die SuisseID bildet das im Jahr 2003 erlassene „Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur", kurz ZertES [SR 943.03, 2008]. Im ZertES werden die Voraussetzungen für die Anerkennung eines Anbieters von Zertifizierungsdiensten im Bereich der elektronischen Signatur festgelegt sowie die Rechte und Pflichten, die ein anerkannter Anbieter hat. Mit dem Gesetz wird bezweckt, ein breites Angebot an sicheren Diensten der elektronischen Zertifizierung zu fördern, den Einsatz qualifizierter elektronischer Signaturen zu begünstigen und die internationale Anerkennung der Anbieter von Zertifizierungsdiensten und deren Leistungen zu ermöglichen.

Das ZertES definiert auch die Begriffe rund um die elektronische Signatur. Erklärt werden die Unterschiede zwischen den drei Qualitätsstufen einer elektronischen Signatur [SR 943.03, 2008: S. 1-2]:

- Eine elektronische Signatur besteht aus elektronischen Daten, die anderen elektronischen Daten beigefügt oder mit ihnen logisch verknüpft sind, und deren Authentifizierung dienen.
- Eine fortgeschrittene elektronische Signatur ist eine elektronische Signatur, die ausschliesslich einem Inhaber zugeordnet ist, und die eine Identifizierung des Inhabers ermöglicht. Sie wird mit Mitteln erzeugt, welche der Inhaber unter seiner alleinigen Kontrolle halten kann. Sie ist mit den Daten so verknüpft, dass eine nachträgliche Veränderung der Daten erkannt wird.
- Eine qualifizierte elektronische Signatur ist eine fortgeschrittene elektronische Signatur, die auf einer sicheren Signaturerstellungseinheit erstellt wurde. Sie beruht auf einem qualifizierten und zum Zeitpunkt der Erzeugung gültigen Zertifikat.

Das ZertES definiert dazu in Artikel 6, welche Anforderungen eine sichere Signaturerstellungseinheit erfüllen muss. Im Zentrum stehen die Einmaligkeit der erzeugten Schlüssel und die Sicherheit vor Fälschungen.

Mit dem Erlass des ZertES wurde eine Reihe bestehender Gesetze angepasst [SR 943.03, 2008: S. 11 ff.]: Auch das für die viele Arten von Verträgen grundlegende Schweizer Gesetz, das Obligationenrecht, kurz OR, wurde an mehrerer Stellen an die Anforderungen der qualifizierten elektronischen Signatur angepasst [SR 220, 2010].

In Bezug auf die SuisseID ist der Gesetzesartikel 14 Absatz 2^{bis} hervorzuheben [SR 220, 2010: S. 4]: Der Absatz regelt die Gleichstellung von ZertES-konformer elektronischer Unterschrift und der Handunterschrift: „Der eigenhändigen Unterschrift gleichgestellt ist die qualifizierte elektronische Signatur, die auf einem qualifizierten Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes vom 19. Dezember 2003 über die elektronische Signatur beruht. Abweichende gesetzliche oder vertragliche Regelungen bleiben vorbehalten."

Die qualifizierte elektronische Signatur ist der handschriftlichen Unterschrift gleichgestellt.

SuisseID-Inhaberhaftung und Sicherheitsvorkehrungen

Darüber hinaus regelt das OR in Artikel 59a die Haftung des Inhabers eines Signaturschlüssels, wie die SuisseID einer ist [SR 220, 2010: S. 17]. Der Artikel legt fest, dass der Inhaber eines Signaturschlüssels für alle Schäden haftet, die einem Dritten entstehen, wenn sich dieser sich auf eine mit dem Signaturschlüssel erstellte qualifizierte Signatur verlässt.

Die Haftung wird nur aufgehoben, wenn der Inhaber des Signaturschlüssels beweisen kann, dass er die notwendigen und zumutbaren Sicherheitsvorkehrungen getroffen hat, um den Missbrauch des Signaturschlüssels zu verhindern. Was für einen Inhaber notwendige und zumutbare Sicherheitsvorkehrungen sind, findet sich auf der SuisseID-Webseite „Empfehlungen zum sicheren Umgang mit der SuisseID" [Staatssekretariat für Wirtschaft SECO, 2010c]. Im November 2010 lauten diese:

- Die SuisseID und die persönliche Identifikationsnummer (PIN) resp. das Passwort müssen immer getrennt aufbewahrt werden.
- Die SuisseID darf nicht einem Dritten übergeben werden.
- Ein Verlust oder Missbrauch der SuisseID muss sofort gemeldet werden. Eine rasche Sperrung (Revozierung) der SuisseID ist zu vollziehen.
- Rechner, auf denen die SuisseID verwendet wird, sind bezüglich Betriebssystem, Anwendungssoftware, SuisseID-Client-Treibersoftware und Virenschutz aktuell zu halten.
- Die SuisseID sollte im Internet nur auf Webseiten eingesetzt werden, denen der Inhaber der SuisseID vertraut.
- Eine SuisseID sollte nach der Verwendung wieder vom Rechner getrennt werden.

Optional empfiehlt das SECO, zur Erhöhung der Anwendungssicherheit einen Smartcard-Leser der Klasse 2 mit eigener Tastatur für die Eingabe der persönlichen Identifikationsnummer einzusetzen. Bei diesen Lesegeräten kann die PIN von einem Dritten nicht ausgelesen werden, selbst wenn der Computer des Anwenders mit einer entsprechenden Schadsoftware infiziert wäre. Weitere Empfehlungen finden sich auf den Webseiten der SuisseID-Anbieter, z.B. auf den Webseiten zur SuisseID der Post [Die Schweizerische Post, 2010a].

Anerkannte Anbieter der SuisseID

Zum ZertES wurden die „Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur“ [SR 943.032, 2005], kurz VZertES und die „Verordnung des BAKOM über Zertifizierungsdienste im Bereich der elektronischen Signatur“ [SR 943.032.1, 2006] erlassen. In den beiden Verordnungen und ihren Anhängen sind im Detail die technischen und administrativen Auflagen beschrieben, die ein Anbieter von Zertifizierungsdiensten erfüllen muss, damit er durch die Schweizerische Akkreditierungsstelle (SAS) des Staatssekretariats für Wirtschaft SECO anerkannt wird.

Auf ihrer Webseite zur Public Key Infrastructure (PKI) publiziert die Schweizerische Akkreditierungsstelle als Abteilung des SECO die Liste der anerkannten Anbieter von Zertifizierungsdiensten [Staatssekretariat für Wirtschaft SECO, 2010a]. Derzeit anerkannte Anbieter von Zertifizierungsdiensten sind Die Swisscom (Schweiz) AG, die QuoVadis Trustlink Schweiz AG, die SwissSign AG der Schweizerischen Post und das Bundesamt für Informatik und Telekommunikation BIT (– die Angaben sind sortiert nach dem Zeitpunkt der Akkreditierung durch die SAS).

Der SuisseID-Standard

Das Staatssekretariat für Wirtschaft SECO und die vier anerkannten Anbieter von Zertifizierungsdiensten lancierten in der zweiten Hälfte des Jahres 2009 das Projekt zur Einführung der SuisseID. Das Projekt wurde im Rahmen der „dritten Stufe der Stabilisierungsmassnahmen“ mit 21 Mio. CHF gefördert. Die konjunkturellen Stabilisierungsmassnahmen wurden vom Bundesrat am 17. Juni 2009 aufgrund der wirtschaftlich schwierigen Lage nach der weltweiten Finanzkrise beschlossen und dem Schweizer Parlament zur Bewilligung empfohlen [Eidgenössisches Volkswirtschaftsdepartement, 2009]. Das Bundesgesetz wurde am 25. September 2009 verabschiedet [SR 951.91, 2009].

Aufbauend auf den Vorgaben des ZertES wurden im Projekt mehrere Ziele verfolgt. Das wichtigste Ziel des Projekts war, die Produkte der vier Anbieter von Zertifizierungsdiensten technisch soweit zu vereinheitlichen, dass sie für einen Nutzer austauschbar sind. Dazu wurden z.B. die Angaben, die ein Anbieter von Zertifizierungsdiensten im Zertifikat zum Signaturschlüssel speichern muss, standardisiert [SR 943.03, 2008: S. 5].

Neben der Vereinheitlichung des Zertifikats für die qualifizierte digitale Signatur wurden Vorgaben für die Ausstellung und Verwendung eines Zertifikats für die Authentisierung von Personen erarbeitet. Dazu wurde eine für alle Anbieter einheitliche SuisseID-Nummerierung geschaffen [Bürge, Zweiacker, 2010: S. 7]. Ein Anbieter einer Anwendung, in der die SuisseID zur Authentisierung verwendet wird, kann diese Nummer zur Erkennung der Nutzer einsetzen. Er muss bei seinem Nutzerkonto lediglich die entsprechende SuisseID-Nummer eintragen. Spezifische oder gar proprietäre Angaben eines Zertifikatsanbieters können durch die Standardisierung vermieden werden.

Zum SuisseID-Standard wurde die technisch gehaltene „SuisseID Specification“ erstellt [Bürge, Zweiacker, 2010]. In der Spezifikation werden die Angaben beschrieben, die in den Zertifikaten für die qualifizierte Signatur und für die Authentifizierung enthalten sein müssen. Es werden die technischen Verfahren beschrieben, mit denen die SuisseID für den Bezug persönlicher Daten in einer Anwendung verwendet werden kann. Weiter wird beschrieben, was der Anbieter einer Anwendung an Technik einsetzen muss, damit er die Funktionen der SuisseID nutzen kann.

Durch die Standardisierung kann der Einsatz der SuisseID immer gleich erfolgen, unabhängig davon, von welchem Anbieter sie stammt.

Im ersten Teil der SuisseID-Spezifikation wird der Aufbau der Zertifikate detailliert beschrieben. Im zweiten Teil wird die Infrastruktur beschrieben, die ein Anbieter von Zertifizierungsdiensten für die SuisseID aufbauen muss. Das sind neben der Public Key Infrastructure (PKI) die für den Einsatz der SuisseID wichtigen Komponenten „Certification Authority“ (CA), „Identity Provider“ (IdP) und „Claim Assertion Service“ (CAS). Das sind die Komponenten, die es dem Inhaber einer SuisseID ermöglichen, sich auf eine sichere und zuverlässige Weise vom Anbieter einer Anwendung authentifizieren zu lassen oder persönliche und bestätigte Daten vorzulegen. Die Infrastruktur, die für den Einsatz der SuisseID notwendig ist, wird in Kapitel „Infrastruktur und Technik hinter der SuisseID“ (S. 31) beschrieben.

Funktionen der SuisseID

Für den elektronischen Identitätsnachweis (Authentifizierung) und die qualifizierte elektronische Unterschrift (Signatur) sind im Chip jeder SuisseID Zertifikate gespeichert, die jeweils einen einmaligen elektronischen Schlüssel enthalten. Im Chip einer SuisseID befindet sich zudem ein kryptografischer Rechner. Dieser Rechner verwendet die auf dem Chip gespeicherten Schlüssel, um Daten zu verschlüsseln oder zu entschlüsseln. Auf diese Schlüssel kann nur dieser kryptografischer Rechner zugreifen. Von aussen ist ein Zugriff auf die Schlüssel nicht möglich. Diese Schlüssel werden auch geheime oder private Schlüssel genannt, denn sie verlassen den Chip nie.

Zu jedem privaten SuisseID-Schlüssel gibt es einen passenden öffentlichen Schlüssel, man spricht auch von asymmetrischer Verschlüsselung. Der öffentliche Schlüssel ist beim Anbieter der SuisseID in der Certification Authority (CA) der Public Key Infrastructure (PKI) gespeichert. Er kann über das Internet von der CA abgerufen werden. Die Funktionsweise des Paares aus privatem und öffentlichem Schlüssel ist, dass Informationen, die mit dem Privaten verschlüsselt wurden, nur mit dem Öffentlichen wieder entschlüsselt werden können. Die Schlüssel können auch umgekehrt verwendet werden: der Öffentliche zum Verschlüsseln und der Private zum Entschlüsseln. Das Paar von öffentlichem und privatem Schlüssel bildet die Basis für die Funktionen der SuisseID.

Elektronischer Identitätsnachweis (Authentifizierung)

Der elektronische Identitätsnachweis mit der SuisseID wird über ein Authentisierungsverfahren erbracht, mit dem die Identität einer Person glaubwürdig festgestellt werden kann. Man stellt bei der Authentisierung fest, ob eine Person die ist, für die sie sich ausgibt. Eine Authentisierung im Bereich der Informatik wird dann notwendig, wenn kontrolliert werden soll, wer auf ein Kommunikationsnetzwerk oder auf die Daten und Funktionen einer Anwendungssoftware zugreift. Die Authentisierung mit der SuisseID ist nur eines von mehreren Verfahren zur Authentisierung (vgl. Kapitel „Andere Authentisierungsverfahren“ S. 38).

Die SuisseID-Authentisierung ist eine „dynamische asymmetrische Authentisierung“. Sie ist das sicherste und somit auch das stärkste aller auf kryptografischen Techniken basierenden Verfahren. Das Verfahren wird auch Challenge-Response-Verfahren genannt [Menezes u. a., 1997: S. 397; Rankl, Effing, 2008: S. 179]. Im Challenge-Response-Verfahren sendet eine erste Instanz der anderen eine zufällig erzeugte Frage, z.B. in Form einer verschlüsselten Zufallszahl (Challenge). Die zweite Instanz berechnet mit einem Algorithmus eine Antwort, z.B. die

entschlüsselte Zufallszahl (Response), und sendet sie der ersten Instanz zur Überprüfung zurück.

Am Beispiel einer SuisseID-basierten Client-Authentisierung an einem Server wird das Verfahren nachfolgend im Detail erklärt (vgl. Abb. 1).

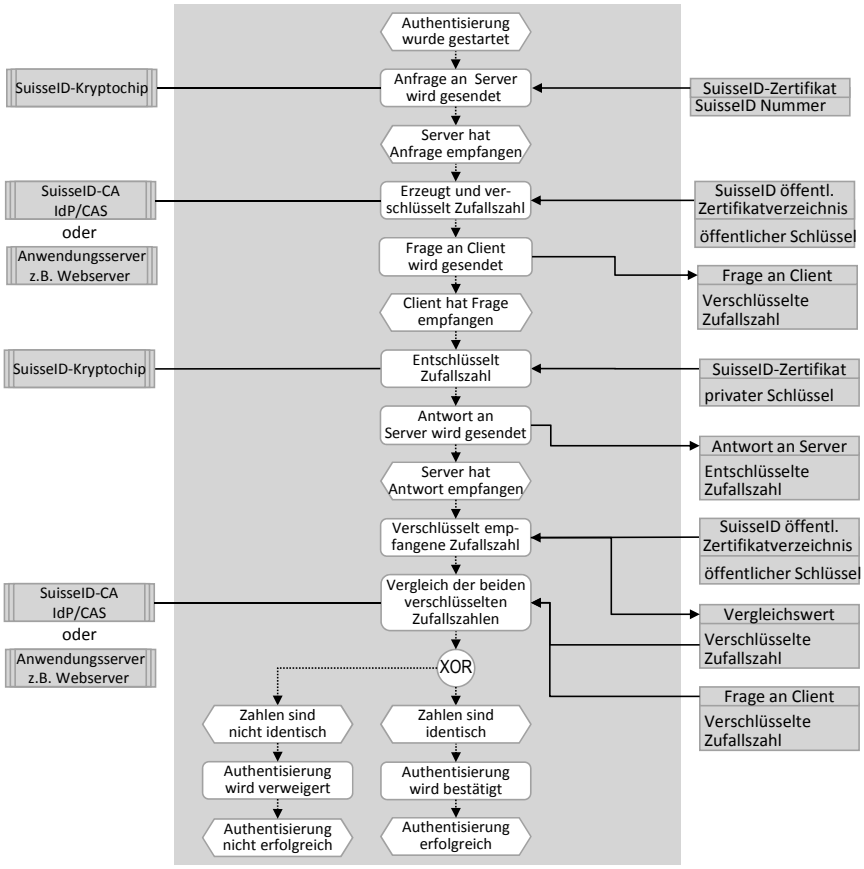


Abb. 1: Dynamische asymmetrische Authentisierung mit der SuisseID

Der Client ist dabei der Kryptochip auf der SuisseID-Chipkarte, ergänzt durch die SuisseID-Client-Treibersoftware, die rein technisch für die Kommunikation mit dem Kryptochip benötigt wird. Der Server ist eine SuisseID-Certification-Authority (CA) mit einem Identity Provider und Claim Assertion Service (IdP/CAS) (vgl. Kapitel „Infrastruktur und Technik hinter der SuisseID“ S. 31).

Das Challenge-Response-Verfahren kann aber auch durch einen Anwendungsserver direkt mit dem SuisseID-Kryptochip ausgeführt werden. Der Anwendungsserver muss dazu den öffentlichen Schlüssel einmalig von

der Certification Authority (CA) bezogen und lokal gespeichert haben. Der Authentisierungsprozess startet mit einer Anfrage des Clients an den Server (vgl. Abb. 1). Mit der Anfrage übermittelt er eine eindeutige Kennung an den Server, im Fall der SuisseID die einmalige SuisseID-Nummer.

Der Server generiert nun eine Zufallszahl. Anhand der empfangenen SuisseID-Nummer holt der Server den passenden öffentlichen Schlüssel hervor und verschlüsselt mit ihm die Zufallszahl. Nun sendet der Server die verschlüsselte Zufallszahl als fiktive Frage – "Wie lautet die entschlüsselte Zufallszahl?" – an den Client.

Der Client entschlüsselt die Zufallszahl mit dem privaten Schlüssel, der auf der SuisseID-Chipkarte gespeichert ist. Die so wieder hergestellte Zufallszahl wird zurück an den Server gesendet.

Der Server überprüft daraufhin die Antwort des Clients. Dazu verschlüsselt er die empfangene Zahl mit dem öffentlichen Schlüssel und vergleicht das Ergebnis mit dem an den Client gesendeten Wert. Sind die beiden Zahlen identisch, so ist die Authentisierung erfolgreich.

Die SuisseID ist eine Zwei-Faktor-Authentisierung. Sie bedingt sowohl den Besitz des Tokens als auch das Kennen des richtigen PINs.

Neben dem Verfahren für die dynamische asymmetrische Authentisierung wird bei der SuisseID eine persönliche Identifikationsnummer (PIN) eingesetzt. Die Authentisierung mit der SuisseID ist daher eine sogenannte „Zwei-Faktor-Authentisierung“: Der erste Faktor ist der „Besitz“ der Chipkarte mit dem privaten Schlüssel und der zweite Faktor die „Kenntnis“ der persönlichen Identifikationsnummer (PIN). Ein Verfahren mit Benutzernamen und Passwort ist hingegen eine weniger sichere „1-Faktor-Authentisierung“. Es ist nur die „Kenntnis“ des Benutzernamens und des Passworts notwendig. (vgl. Kapitel „Andere Authentisierungsverfahren“ S. 38).

Die Zwei-Faktor-Authentisierung mit der SuisseID wird in den nachfolgend beschriebenen Varianten eingesetzt.

Einfache Authentisierung

Das Verfahren der einfachen Authentisierung wird vor allem für die Anmeldung von Nutzern bei Anwendungen verwendet. Bei der einfachen Authentisierung mit der SuisseID sind drei Rollen mit ihren Informationssystemen beteiligt. Der Anbieter mit einem Anwendungsserver, der SuisseID-Anbieter mit seiner Public Key Infrastructure (PKI) und der Nutzer mit dem Anwendungs-Client und seiner SuisseID. Abb. 2 zeigt die

drei Rollen mit ihren Informationssystemen am Beispiel eines Onlineshops und dessen Kunden.

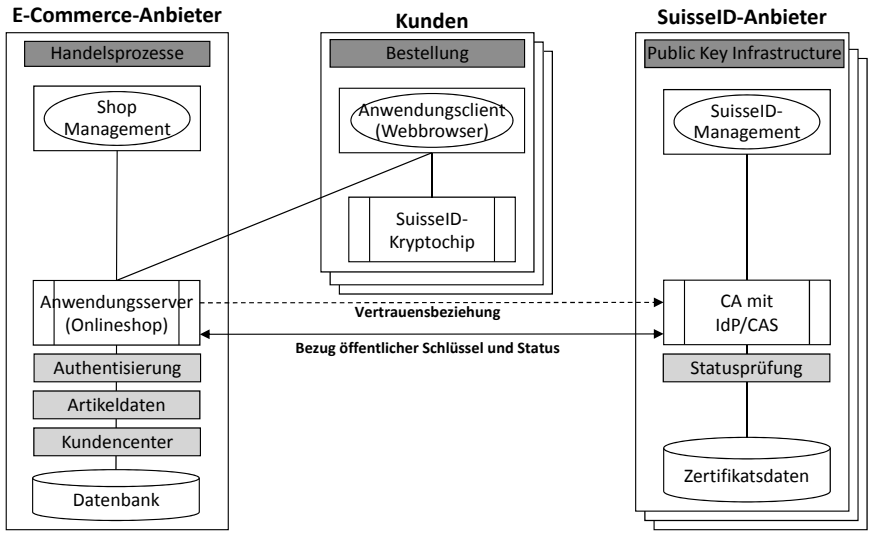


Abb. 2: Informationssysteme bei der einfachen Authentisierung

Das Informationssystem, das beim SuisseID-Anbieter für die einfache Authentisierung eingesetzt wird, ist die Certification Autority mit dem Verzeichnis der Zertifikate. Die CA kommuniziert mit der Anwendung des Anbieters während der Authentisierung. Die Anwendung bezieht den öffentlichen Schlüssel und prüft bei der CA die Gültigkeit der SuisseID. Der Bezug des öffentlichen Schlüssels durch die Anwendung ist nur notwendig, wenn die Anwendung diesen nicht bereits bezogen und lokal gespeichert hat.

Der Prozess der einfachen Authentisierung startet damit, dass der Nutzer eine Anwendung nutzen möchte und von dieser Anwendung eine Anmeldung verlangt wird (vgl. Abb. 3). Die erste Aktivität des Nutzers ist die Wahl der Anmeldung mit einer SuisseID in seinem Anwendungs-Client (z.B. in einer auf seinem Rechner installierten Anwendungssoftware oder in einer Anwendung im Webbrowser). Dabei kann der Nutzer möglicherweise zwischen verschiedenen Authentisierungsverfahren wählen.

Der Rechner des Nutzers prüft, ob eine SuisseID-Chipkarte am Rechner angeschlossen ist. Ist das nicht der Fall, wird die Anmeldung abgebrochen und eine Fehlermeldung angezeigt. Ist eine SuisseID angeschlos-

sen, wählt der Nutzer das SuisseID-Authentisierungszertifikat aus, sofern dieser Schritt nicht automatisch erfolgt.

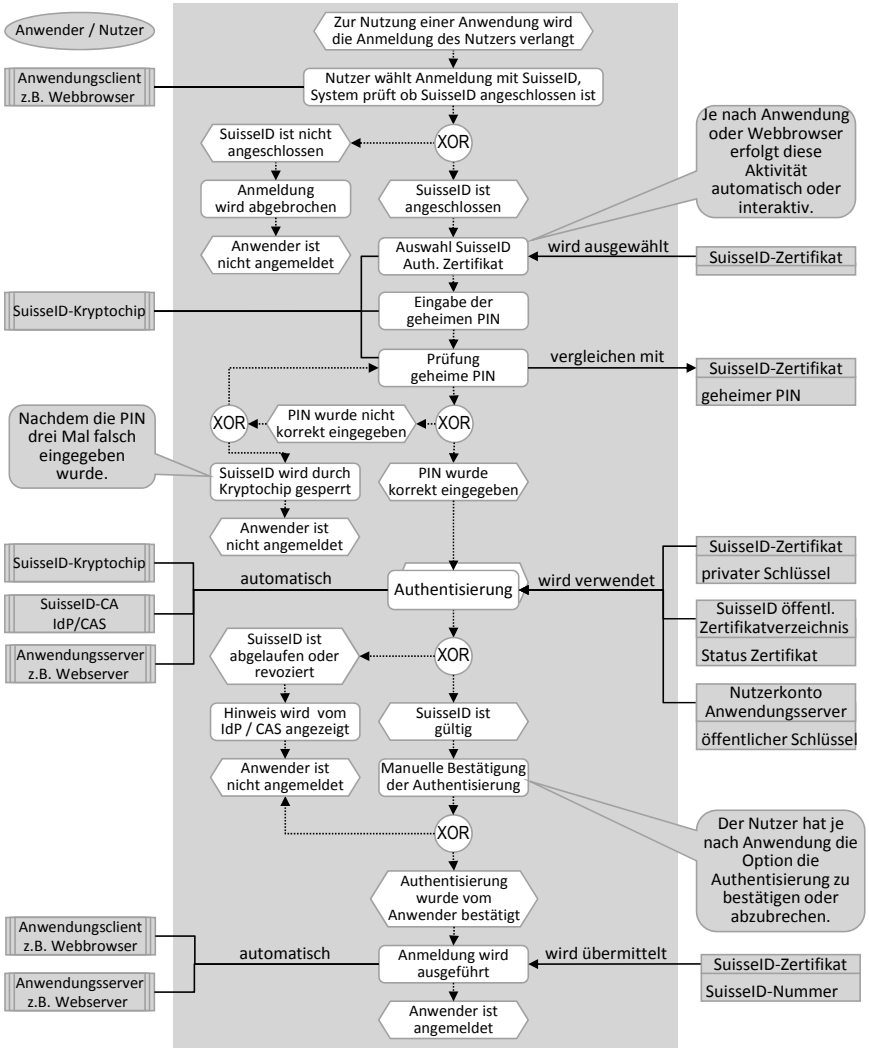


Abb. 3: Prozess einfache Authentisierung

Danach wird der Nutzer aufgefordert, seine geheime persönliche Identifikationsnummer (PIN) einzugeben. Der PIN kann auch alphanummerisch sein, d.h. ein Passwort aus beliebigen Zeichen. Der Nutzer hat drei Versuche, die PIN resp. das Passwort korrekt einzugeben. Nach dem dritten Fehlversuch sperrt der Kryptochip auf der SuisseID den Zugriff auf die Chipkarte. Nach einer Sperrung kann eine SuisseID nicht weiter eingesetzt werden, sie kann auch nicht mehr entsperrt werden. Wurde

die PIN korrekt eingegeben, wird die Authentisierung gestartet. Sie läuft nach dem Verfahren der dynamischen asymmetrischen Authentisierung ab (vgl. Abb. 1).

Danach wird dem Nutzer angezeigt, ob die Authentisierung erfolgreich durchgeführt werden konnte oder nicht. Ist die verwendetet SuisseID abgelaufen oder wurde sie für ungültig erklärt (revoziert), wird dem Nutzer je nach Anwendung eine Fehlmeldung angezeigt. Bei erfolgreicher Authentisierung kann es sein, dass der Nutzer zur Bestätigung der Authentisierung aufgefordert wird. Je nach Anwendung wird dieser Schritt auch übersprungen und der Nutzer wird gleich nach erfolgreicher Authentisierung am Anwendungsserver angemeldet.

Die einfache Authentisierung wird in allen vier in diesem Buch beschriebenen Anwendungsfällen eingesetzt. Bei den Fallstudien zu buch.ch (S. 65) und elektronische Service Plattform (S. 41) wird für die erstmalige Registrierung von Nutzern auch das im Folgenden beschriebene Verfahren eingesetzt.

Authentisierung mit Nachweis von identifizierenden Merkmalen

Die Authentisierung mit Nachweis von identifizierenden Merkmalen ist eine Erweiterung der einfachen Authentisierung. Bei dieser Authentisierung werden zusätzlich Daten über den Claim Assertion Service (CAS) der SuisseID-Anbieter angefordert.

Der Begriff Claim Assertion Service bedeutet so viel wie „Bestätigungsdienst für identifizierenden Merkmale“. Gemeint sind Merkmale, anhand deren ein Inhaber einer SuisseID eindeutig identifiziert werden kann. Die Merkmale, die in über einen CAS bezogen werden können, sind verifizierte Angaben, d.h. der Anbieter der SuisseID musste diese Angaben bei jeder Bestellung einer SuisseID vom Besteller erheben.

Der Nutzer kann in jedem einzelnen Fall über die Weitergabe identifizierender Merkmale entscheiden und bei Bedarf auch einzelne Angaben verweigern.

Der Nachweis von identifizierenden Merkmalen eignet sich besonders für die Registrierung von neuen Nutzern, z.B. wenn sich ein Kunde in einem Onlineshop neu registrieren möchte, und bisher keine Geschäftsbeziehung bestand. Diese Art der Authentisierung ist auch geeignet, wenn ein Vertrag online abgeschlossen werden soll. Z.B. bei Verträgen zwischen Endkunden und Unternehmen, wenn sich der Endkunde mit einem Ausweis identifizieren muss.

Bei der SuisseID sind die identifizierenden Merkmale die Angaben aus dem offiziellen Ausweisdokument, das bei der Bestellung der SuisseID

zur Identifizierung des zukünftigen SuisseID-Inhabers verwendet wurde. Die in Tab. 1 aufgeführten Angaben werden als identifizierende Merkmale beim SuisseID-Anbieter gespeichert.

Tab. 1: Identifizierende Merkmale, die beim SuisseID-Anbieter gespeichert sind

Angaben zur Person	Angaben zum verwendeten Ausweis
Geschlecht (männlich oder weiblich)	Art des Ausweises (Pass oder ID)
Vorname, Nachname	Nummer des Ausweises
Geburtsdatum	Ausstellungsland
Alter über 18	Ausstellende Behörde
Bürgerort (bei Schweizern)	Ausstellungsdatum
Geburtsort (bei Ausländern)	Ablaufdatum

Bei der Authentisierung mit Nachweis von identifizierenden Merkmalen kommen dieselben Informationssysteme zum Einsatz wie bei der einfachen Authentisierung (vgl. Abb. 4). Der Prozess ist nutzerzentrisch gestaltet, d.h. ein Nutzer kann jederzeit bestimmen, angeforderte Daten weiterzugeben oder den Prozess der Anmeldung abzubrechen. Der Austausch von persönlichen Nutzerdaten zwischen dem Anwendungsserver und dem SuisseID-Anbieter läuft immer über den Anwendungsclient.

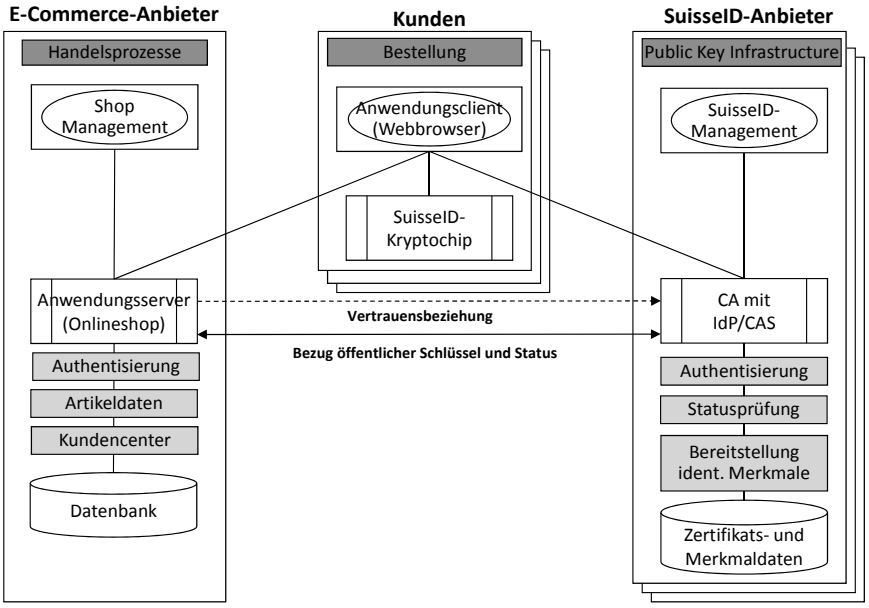


Abb. 4: Informationssysteme bei Authentisierung mit identifizierenden Merkmalen

Ein Anbieter einer Anwendung muss festlegen, welche Merkmale er für seine Zwecke benötigt. Dabei steht es ihm frei, einige Merkmale als zwingend und andere als optional zu fordern. Optionale Merkmale kann ein Nutzer vor der Übermittlung an die Anwendung abwählen. Die Verweigerung zwingender Merkmale führt zum Abbruch der Authentisierung.

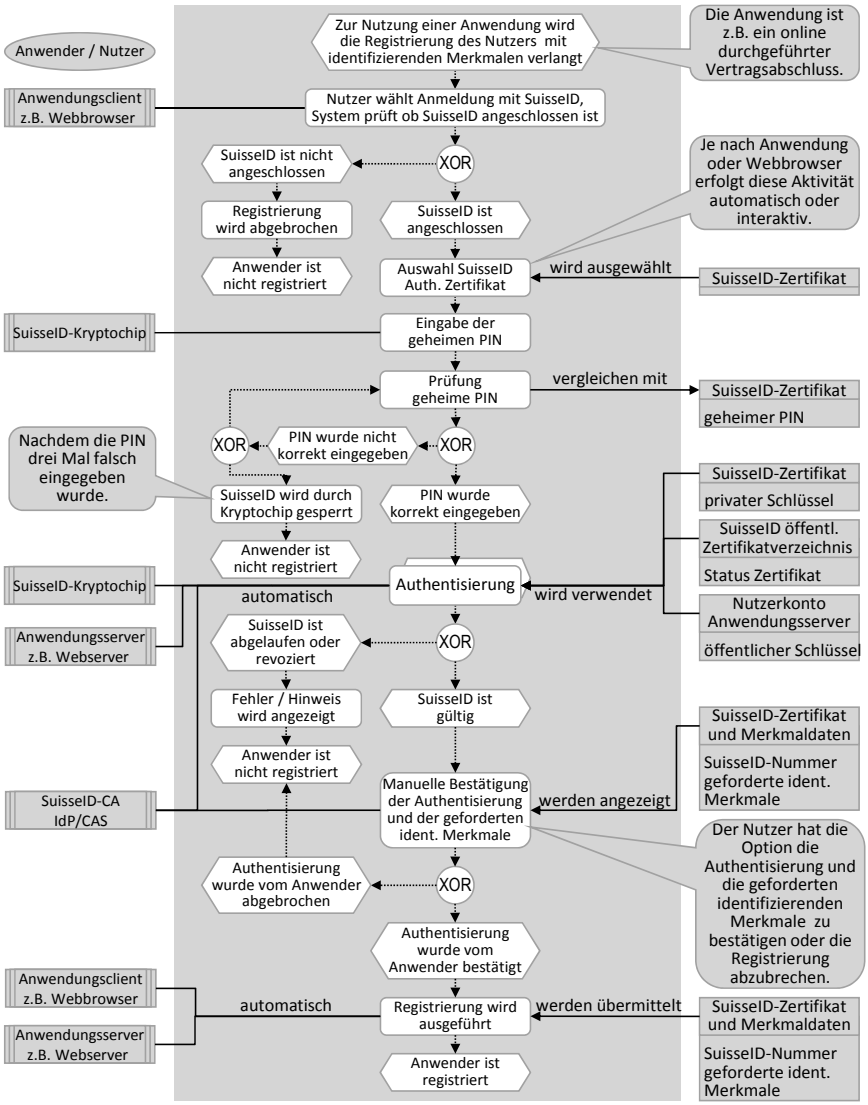


Abb. 5: Authentisierung mit Nachweis von identifizierenden Merkmalen

Der Prozess wird am Beispiel einer Registrierung bei einer Anwendung aufgezeigt (vgl. Abb. 5). Er unterscheidet sich nur an wenigen Stellen von der einfachen Authentisierung. Der Prozess startet damit, dass eine Anwendung für die Registrierung identifizierende Merkmale verlangt. Die Forderung nach identifizierenden Merkmalen ist bereits in der Funktion hinterlegt, die der Nutzer im Anwendungsclient für die Registrierung ausführen muss.

Wie bei der einfachen Authentisierung wird das Vorhandensein einer SuisseID geprüft, die persönliche Identifikationsnummer (PIN) abgefragt und die Gültigkeit der SuisseID kontrolliert. Sind alle diese Schritte erfolgreich abgeschlossen, wird dem Nutzer eine Seite mit den von der Anwendung geforderten Merkmalen angezeigt (vgl. Abb. 3 in Fallstudie buch.ch, S. 71). Der Nutzer kann nun die Übermittlung der geforderten Merkmale an die Anwendung auslösen oder abbrechen, sollte er die Merkmale nicht preisgeben wollen.

Die Authentisierung mit Nachweis von identifizierenden Merkmalen wird primär für die Erstregistrierung von Kunden oder Geschäftspartnern eingesetzt. Bei buch.ch kommt dieses Verfahren auch bei bestehenden Kunden zum Einsatz, wenn sie sich erstmalig mit ihrer SuisseID im Onlineshop anmelden möchten. Ein bestehender Kunde hat die Möglichkeit, seine SuisseID mit dem seinem Kundenkonto zu verbinden.

Authentisierung mit Nachweis von zusätzlichen Merkmalen

Die Authentisierung mit Nachweis von zusätzlichen Merkmalen ist im Grunde das gleiche Verfahren wie die Authentisierung mit Nachweis von identifizierenden Merkmalen. Der Unterschied liegt darin, dass die zusätzlichen Merkmale nicht bei einem SuisseID-Anbieter gespeichert sind, sondern auf einem Claim Assertion Service (CAS) eines Dritten, einem sogenannten Bestätigungsanbieter (vgl. Abb. 6).

Durch zusätzliche Merkmale, die auch von neuen Anbietern bereitgestellt werden können, ist das System der SuisseID flexibel erweiterbar.

Ein Bestätigungsanbieter stellt beliebige zusätzliche Merkmale bereit. Z.B. Funktionen, die eine Person ausüben darf, wie etwa praktizierender Arzt, Notar oder Prokurist. Auch andere personenbezogene Merkmale sind möglich wie z.B. die Wohnadresse, Bankverbindung oder Telefonnummer. Sollte es sich bei derartigen Merkmalen um Daten handeln, die dem Datenschutz unterliegen, muss ein Bestätigungsanbieter die entsprechenden Auflagen aus dem Datenschutzgesetz einhalten [SR 235.1, 2008].

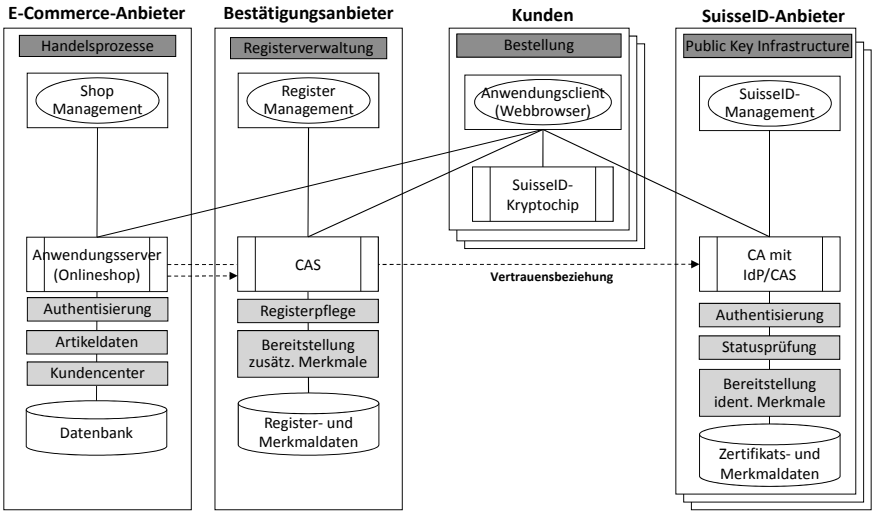


Abb. 6: Informationssysteme bei Authentisierung mit zusätzlichen Merkmalen

Qualifizierte elektronische Unterschrift (Signatur)

Unter einer qualifizierten elektronischen Signatur ist nicht etwa die Signatur gemeint, die in vielen E-Mail-Anwendungen als Absenderangabe unterhalb eines Textes angehängt werden kann. Eine qualifizierte elektronische Signatur funktioniert mehr wie ein Wachssiegel auf einem Briefumschlag oder eine Plombe an einem Frachtcontainer: Solange das Siegel oder die Plombe unversehrt ist, ist sichergestellt, dass der Inhalt unverändert ist.

Die qualifizierte elektronische Unterschrift ist der handschriftlichen Unterschrift gleich gestellt. Sie hat gegenüber dem Gesetz die gleiche Gültigkeit (vgl. Kapitel „Gesetzliche Rahmenbedingungen“ S. 14). Der wesentliche Unterschied zwischen handschriftlicher und digitaler Unterschrift ist, dass die handschriftliche auf einem Papierdokument, und die digitale auf einem elektronischen Dokument aufgebracht wird. Handschriftliche Unterschriften sind nur auf den jeweiligen Originaldokumenten gültig, eine Kopie eines handschriftlich unterschriebenen Papierdokuments ist nicht gültig. Digitale Signaturen sind hingegen auf allen elektronischen Kopien eines elektronischen Dokuments gültig, solange der Inhalt des Dokuments nicht verändert wurde, d.h. die Integrität des Inhaltes gewahrt ist. Wird jedoch ein digital unterschriebenes Dokument ausgedruckt, verliert die digitale Signatur ihre Gültigkeit. Denn in diesem Fall kann nicht mehr verifiziert werden, ob der Inhalt des Dokuments unverändert ist, und ob die Signatur zum Zeitpunkt der Erstellung gültig

war. Die Gültigkeit einer digitalen Signatur kann nur überprüft werden, solange das signierte Dokument in elektronischer Form vorliegt.

Die Informationssysteme, die für den Einsatz der qualifizierten elektronischen Signatur benötigt werden, sind in Abb. 7 dargestellt. Danach signieren Nutzer aus Unternehmen 1 mit ihrer SuisseID und einer Signaturanwendung z.B. Verträge. In Unternehmen 2 prüfen die Nutzer die von Unternehmen 1 empfangenen Verträge ebenfalls mit einer Signaturanwendung.

Mit einer Signaturanwendung kann i.d.R. eine qualifiziert elektronische Signatur erstellt und geprüft werden. Eine weitverbreitete Signaturanwendung ist z.B. der kostenlose Adobe Reader [Adobe Systems Inc., 2010a]. Mit dem Adobe Reader können Dokumente im Portable Document Format (PDF) signiert werden, wenn sie als Formular gestaltet sind und ein spezielles Unterschriftsfeld enthalten. Mit dem kostenpflichtigen Adobe Acrobat können beliebige PDF Dokumente signiert werden [Adobe Systems Inc., 2010b]. Eine andere Signaturanwendung ist SwissSigner vom SuisseID-Anbieter SwissSign. Mit dem SwissSigner können ebenfalls beliebige PDF Dokumente und auch bestimmte Bildformate signiert werden. SwissSigner wird in zwei Varianten angeboten. Eine kostenlose Version für alle Inhaber einer Post SuisseID und eine kostenpflichtige Version, die auch mit einer SuisseID von anderen Anbietern genutzt werden kann [SwissSign AG, 2010a].

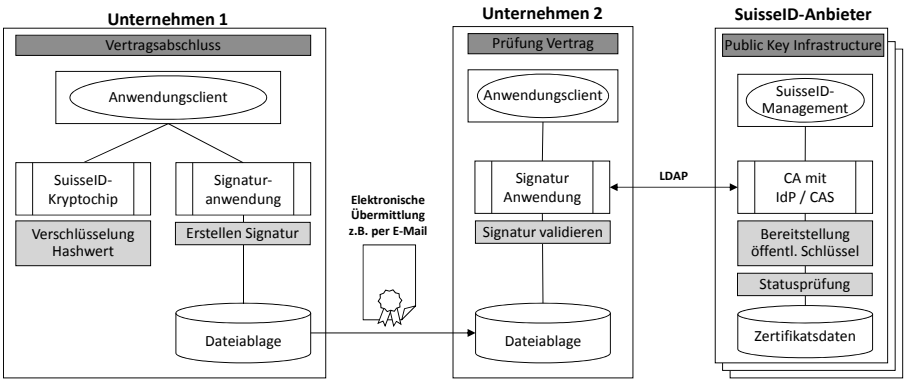


Abb. 7: Informationssysteme beim Einsatz qualifizierter elektronischer Signaturen

PDF-Dokumente sind besonders geeignet für den Einsatz der qualifizierten elektronischen Signatur, da sie auf allen aktuellen Betriebssystemen genutzt werden können.

Neben PDF-Dokumenten können auch andere Dokumente mit einer Signatur versehen werden. Es hängt von der eingesetzten Signaturanwendung ab, welche Dokumentformate unterstützt werden. Häufig werden E-Mail-Nachrichten mit einer elektronischen Signatur versehen. Gegenüber anderen Dokumentformaten ist es bei E-Mail-Nachrichten nicht möglich, dass mehrerer Personen signieren. Beim Signieren von E-Mail-Nachrichten gilt es in erster Linie, die Identität des Absenders zu belegen. Dazu empfehlen die SuisseID-Anbieter die Verwendung des Authentisierungszertifikats. Das Zertifikat für qualifizierte digitale Signatur ist nur dann zwingend zu verwenden, wenn rechtsgültige Geschäfte getätigt werden.

Für die Prüfung einer qualifizierten elektronischen Signatur wird der öffentliche Schlüssel benötigt, der zu derjenigen SuisseID passt, die für das Erstellen der Signatur verwendet worden ist. Dazu greift die Signaturanwendung auf das Certificate Authority (CA) des entsprechenden SuisseID-Anbieters zu. Der Zugriff auf die CA erfolgt mit dem Lightweight Directory Access Protocol (LDAP), ein gängiges Protokoll für die Abfrage von Informationen aus Verzeichnissen.

Erstellung einer digitalen Signatur

Der Prozess des digitalen Signierens beginnt damit, dass ein elektronisches Dokument vorliegt, das signiert werden soll (vgl. Abb. 8).

In der Signaturanwendung wird durch den Nutzer die Funktion zur Erstellung der qualifizierten elektronischen Signatur gestartet. Über die SuisseID-Client-Treibersoftware wird geprüft, ob eine SuisseID am Rechner angeschlossen ist. In diesem Fall wird die PIN resp. das Passwort abgefragt und mit der auf der SuisseID gespeicherten PIN verglichen. Stellt der Vergleich eine Übereinstimmung fest, beginnt die Erstellung der Signatur mit der Berechnung des Hashwertes.

Eine gültige digitale Signatur sagt aus, dass der Inhalt des Dokuments nicht verändert wurde. Handelt es sich um eine fortgeschrittene digitale Signatur, wird zusätzlich die Person, von der die Signatur stammt, identifiziert. Eine qualifizierte digitale Signatur macht zusätzliche Aussagen zur Qualität des Zertifikats.

Von dem zu signierenden Vertrag (z.B. ein PDF-Dokument) wird mit dem Secure Hash Algorithm (SHA) der Hashwert des Dokumentinhalts berechnet. Man kann sich den mit SHA berechneten Hashwert als Fingerabdruck des Dokuments vorstellen, denn er ist mit sehr hoher Wahrscheinlichkeit einzigartig. Der Hashwert wird nun mit dem privaten SuisseID-Schlüssel im Kryptochip der SuisseID verschlüsselt und mit Informationen aus dem Zertifikat als qualifizierte elektronische Signatur an das Dokument angefügt. Der Vertrag ist somit signiert. Der Hashwert

kann nun ausschliesslich mit dem passenden öffentlichen SuisseID-Schlüssel entschlüsselt werden.

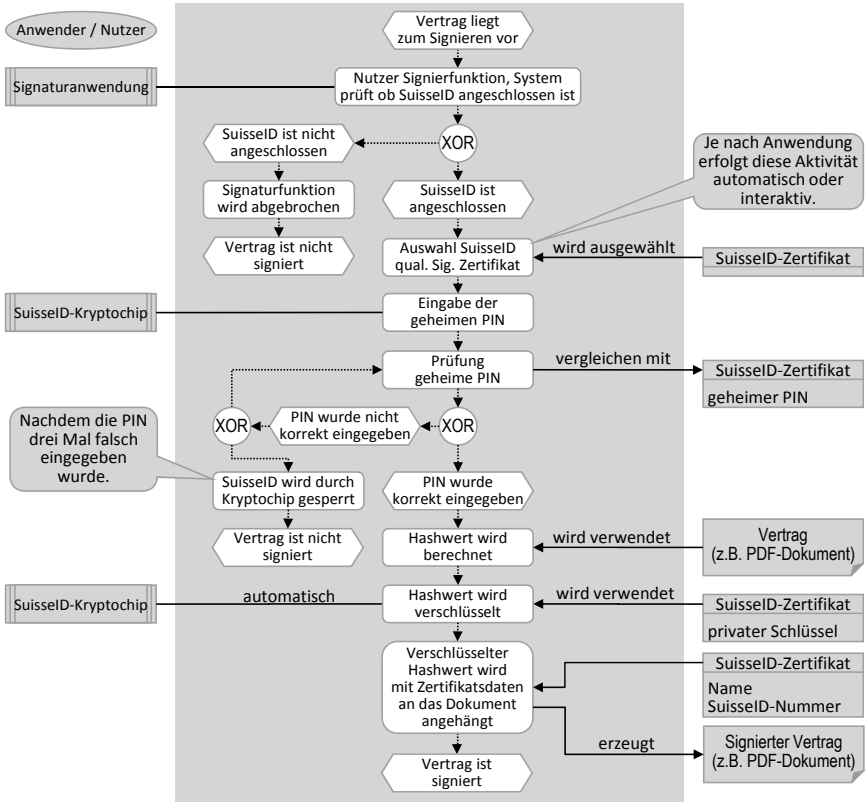


Abb. 8: Prozess digitales Signieren eines Dokuments

Prüfung einer digitalen Signatur

Der Nutzer, der die Signatur auf ihre Gültigkeit prüfen will, öffnet den signierten Vertrag in einer Signaturanwendung (vgl. Abb. 9). Die Signaturanwendung muss dabei nicht derjenigen entsprechen, wie die zur Erstellung der Signatur verwendet wurde. Zur Prüfung der Gültigkeit wird wiederum der Hashwert des Dokuments berechnet. Der passende öffentliche Schlüssel wird vom öffentlichen Zertifikatsverzeichnis abgerufen. Der in der Signatur gespeicherte Hashwert wird entschlüsselt und mit dem neu berechneten verglichen. Die digitale Signatur ist gültig, wenn die beiden Hashwerte identisch sind. Damit zeigt sich, dass der Dokumentinhalt seit dem Signieren nicht verändert wurde. Bei identischen Hashwerten wird anhand des Zertifikatsverzeichnisses geprüft, ob die bei der Erstellung der Signatur verwendete SuisseID gültig war. Am

Ende des Prüfungsprozesses wird dem Nutzer angezeigt, ob die Signatur gültig ist oder aus welchem Grund die Gültigkeit ggf. nicht festgestellt werden konnte.

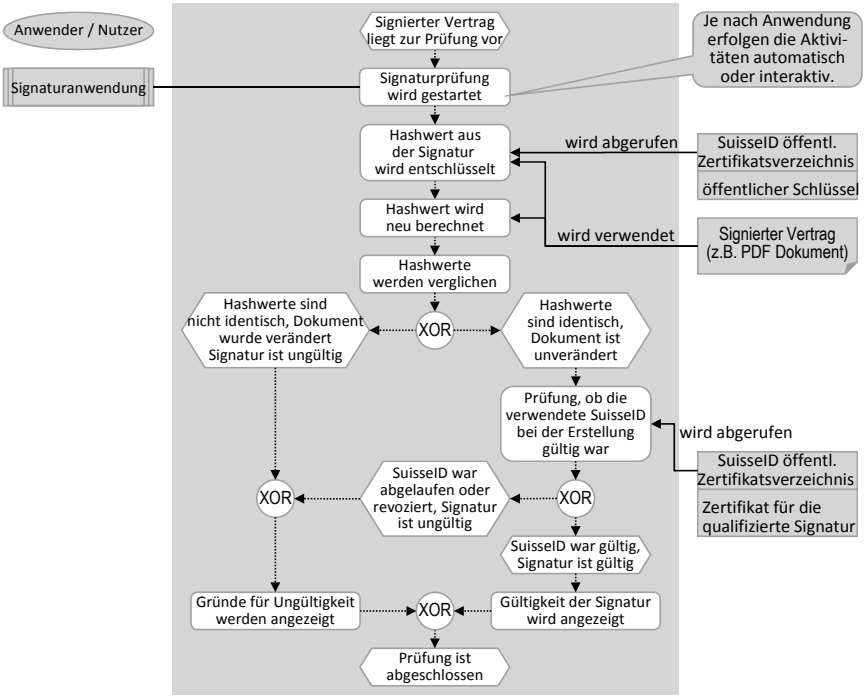


Abb. 9: Prozess prüfen einer digitalen Signatur

Infrastruktur und Technik hinter der SuisseID

Die Infrastruktur und Technik hinter der SuisseID basiert auf dem Prinzip der Public Key Infrastructure (PKI) nach dem X.509 Standard [ITU-T Recommendation, 2005]. Eine PKI beinhaltet alle notwendigen Betriebs- und Verwaltungseinrichtungen, die für einen auf asymmetrischer Verschlüsselung basierenden Informationsaustausch benötigt werden.

Zu den Einrichtungen gehören typischerweise Registrierungsstellen (Registration Authority, RA), Zertifizierungsinstanzen (Certificate Authority, CA) sowie Verzeichnisdienste.

Bei den SuisseID-Anbietern können die Registrierungsstellen (RA) auch Dritte sein. Bei der Post SuisseID können sich beispielsweise Personen, die über das Internet eine SuisseID bestellt haben, am Postschalter iden-

tifizieren lassen. Die SuisseID-Anbieter selbst stellen die Certificate Authority (CA). Sie betreiben die Zertifikatsverzeichnisse und stellen die SuisseID aus. Die für die SuisseID benötigte wichtigsten Einrichtungen werden in Abb. 10 gezeigt [Bürge, Zweiacker, 2010: S. 19 ff.].

Auf Basis der CA betreiben die SuisseID-Anbieter die zentralen Dienste Identity Provider (IdP) und Claim Assertion Service (CAS). Ein IdP wird für die Authentisierung mit der SuisseID eingesetzt, ein CAS für die Bereitstellung von identifizierenden Merkmalen (vgl Kapitel „Authentisierung mit Nachweis von identifizierenden Merkmalen“, S. 23). Beide Dienste können auf demselben Informationssystem betrieben werden.

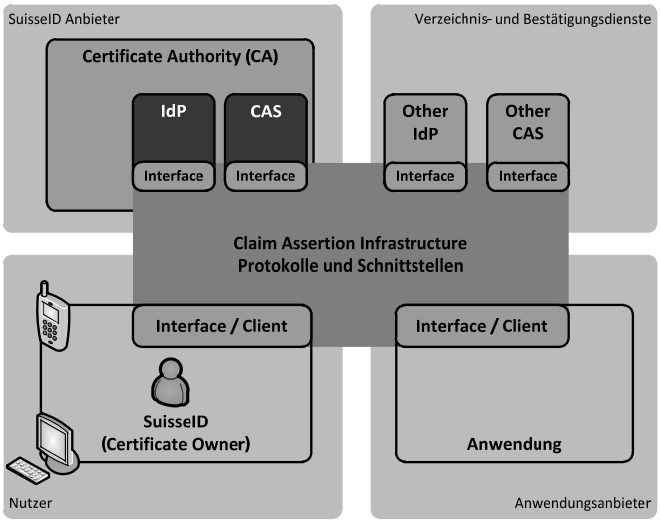


Abb. 10: SuisseID Infrastruktur [in Anlehnung an Bürge, Zweiacker, 2010: S. 19]

Für die Bereitstellung dieser beiden Dienste im Rahmen von Authentisierungsverfahren mit der SuisseID wird die Claim Assertion Infrastructure eingesetzt. Die Claim Assertion Infrastructure basiert auf definierten Protokollen und Schnittstellen, die alle SuisseID-Anbieter einsetzen müssen.

Der SuisseID-Standard nutzt für den Austausch von Nachrichten die „Security Assertion Markup Language“ (SAML) in der Version 2.0. SAML basiert auf der Extensible Markup Language (XML) und wurde speziell für den Austausch von Informationen in Authentisierungsverfahren entwickelt [Cover, 2010].

SuisseID-Produktvarianten

Die SuisseID wird von den SuisseID-Anbietern als Produkt in unterschiedlichen Varianten angeboten. Die aktuellen Varianten basieren i.d.R. auf einem Kryptochip, der auf eine Kunststoffkarte in Form einer Kreditkarte oder in Form einer SIM-Karte aufgebracht ist (Formate ID-01 und ID-000 nach ISO/IEC 7816-1 [1998]). Bei der Bestellung einer SuisseID kann die gewünschte Variante ausgewählt werden.

Je nach Variante werden unterschiedliche Lesegeräte benötigt. Ein passendes Lesegerät kann bei der SuisseID-Bestellung mitgeordert werden (vgl. Abb. 11). Die aktuell mitgelieferten Lesegeräte entsprechen der Klasse 1 und besitzen keinen PIN-Pad (Zahlenblock-Tastatur). Der PIN muss dementsprechend über die Tastatur des Computers eingegeben werden, was im Fall von kompromittierten Geräten ein Sicherheitsrisiko darstellen kann. Die Lesegeräte werden über eine USB-Schnittstelle an einen Rechner angeschlossen. Damit die Lesegeräte verwendet werden können, muss eine SuisseID-Client-Treibersoftware entsprechend dem genutzten Betriebssystem installiert sein. Die SuisseID-Client-Treibersoftware wird durch die SuisseID-Anbieter im Internet bereitgestellt.

Abb. 11: SuisseID im Kreditkartenformat- und im SIM-Format mit entsprechenden Lesern

Anstatt eines Kartenlesers, der über die USB-Schnittstelle angeschlossen wird, kann auch ein in den Rechner eingebauter Leser verwendet werden. Solche Leser sind z.B. in aktuellen Business-Notebook-Modellen verschiedener Hersteller eingebaut.

Eine weitere Produktvariante wird vom SuisseID-Anbieter SwissSign in Form des „SwissStick“ angeboten [SwissSign AG, 2010b]. Der SwissStick ist ein intelligenter USB-Memorystick inklusive Anwendungssoftware (vgl. Abb. 12). Im SwissStick ist die Post SuisseID in Form einer SIM-Karte eingebaut.

Auf dem SwissStick stehen verschiedene Anwendungen zur Verfügung. Sie können nach dem Verbinden des SwissStick mit einem Rechner ohne Installation genutzt werden. Die auf dem SwissStick installierten Anwendungen sind die Signatursoftware SwissSigner (vgl. Kapitel „Qualifizierte elektronische Unterschrift (Signatur)“ S. 27) und der IncaMail-Client für die sichere und nachweisbare elektronische Kommunikation [Die Schweizerische Post, 2010b]. Weiter vorhanden ist ein Webbrowser: Mit ihm kann sicher im Internet gesurft werden, ohne auf dem benutzten Rechner Spuren zu hinterlassen, denn bei der Nutzung des SwissStick werden dort keine Dateien gespeichert.

Abb. 12: SwissStick von SwissSign mit der Post SuisseID

SwissSign bietet einen Update Service, der gewährleistet, dass die auf dem SwissStick gespeicherten Anwendungen immer aktuell sind. Der SwissStick unterstützt die Betriebssysteme von Microsoft (ab Windows XP SP2) und Apple (Mac OS X ab 10.5).