verimi

Sicherheit Verimi

Übersicht über Sicherheitsfunktionen einer industrieübergreifenden Identitätsplattform

Februar 2021
White Paper

V1.2

Inhalt

Abstract

Gegenwärtig hinterlassen Nutzer im digitalen Raum umfangreiche Spuren, die anders als in der analogen Welt prinzipiell in Form von Daten verfügbar bleiben. Dieses Exponieren von Nutzerdaten trifft auf strukturell unsichere technologische Paradigmen und ermöglicht vielfältigen Missbrauch. An dieser Stelle setzt Verimi an und bietet auf Basis sicherer Technologie-Ansätze sicheres Identitätsmanagement, um Nutzern genauso wie Unternehmen und Behörden die Möglichkeit technologischer Emanzipation, d.h. sicherer Inter- und Transaktion an die Hand zu geben.

Das vorliegende White Paper legt nach einer kurzen Einleitung die relevanten Sicherheitsaspekte von Verimi offen: mit Blick auf die verfügbaren Funktionen, die technologischen Dimensionen sowie schließlich die Ablauf- und Aufbauorganisation. Wir verstehen das Papier darüber hinaus als Beitrag zur übergeordneten fachlichen Diskussion von Sicherheitsthemen und begrüßen jede konstruktive Kritik ausdrücklich und stellen dafür die folgende Adresse zur Verfügung: security@verimi.com.

1 Einleitung

Geschäftsmodelle im digitalen Raum basieren in weiten Teilen auf der Sammlung, Auswertung und Nutzung von Daten, die Nutzer bereitstellen bzw. die über sie gewonnen werden können. Dies ermöglicht Unternehmen, kontextbezogen und nutzerspezifisch – d.h. möglichst differenziert – zu agieren und Mehrwert für Nutzer zu schaffen. Für diese Geschäftsmodelle können personenbezogene Daten indirekt erhoben werden, was jedoch in einem zunehmenden Umfang für weitergehende Geschäftsaktivitäten keine ausreichende Grundlage für das Grundgeschäft darstellt. Hier sind in fortschreitendem Maße personenbezogene Daten verfahrenstechnisch (B2B2C, End-to-End) oder aus regulatorischen Gründen (Anti Money Laundering AML, Know your Customer KYC) heranzuziehen, deren Herkunft oder Aktualität geeignet nachzuweisen sind.

Neben den Potenzialen bergen verwendete Verfahren und Technologien Möglichkeiten des Missbrauchs, wie der Anstieg der Sicherheitsvorfälle[1] der vergangenen Jahre vor Augen führt. Zwar sind Spezialanbieter führend in der Entwicklung höchster Sicherheitsstandards, viele Marktteilnehmer verfügen jedoch weder über die Mittel noch die Kompetenz, diese Standards umzusetzen. Zudem sind Herausforderungen der Nutzerfreundlichkeit für sichere Verfahren nach wie vor nicht befriedigend gelöst, womit Akzeptanzwerte trotz mittlerweile fortschreitender Aufklärung auf niedrigem Niveau verharren.

Die notwendige Erhöhung und Aufwertung der Sicherheit sowie der individuell abgesicherte Einsatz von personenbezogenen Daten im digitalen Raum sind unumstritten. Ein mehrschichtiger Ansatz zielt auf eine systematische Stabilisierung: durch Schutz der Privatsphäre (Datenschutz-Grundverordnung DSGVO, ePrivacy), Stärkung des Vertrauens in digitale Instrumente (z.B. eIDAS[2]) und die Einhaltung

[1] Mehr als eine Verfünffachung der weltweiten Vorfälle zwischen 2013 und 2017, siehe [11] und [12].
[2] electronic Identification, Authentication and Trust Services.

technologischer (Sicherheits-)Standards (IT-Sicherheitsgesetz ITSiG u.a.). Ein Interessenausgleich unter wirtschaftlicher, staatlicher und zivilgesellschaftlicher Beteiligung ist flankierend anzustreben.

Verimi setzt an der Schnittmenge der Lösungselemente an und etabliert eine Identitätsmanagement-Plattform für sichere elektronische Identitäten als Grundlage für rechtskonforme und vertrauenswürdige Geschäftsprozesse im Internet. Ziel von Verimi ist, das Identitätsmanagement für Nutzer, Unternehmen und Behörden sicher, benutzerfreundlich und datenschutzkonform umzusetzen. Dabei bildet Verimi die Schnittstelle zwischen Nutzern auf der einen und Anwendungspartnern (Unternehmen und Behörden) auf der anderen Seite.

Die für verschiedene Services benötigten personenbezogenen Daten werden innerhalb der Verimi-Plattform sicher und für den Nutzer transparent verwaltet. Nutzer, die Services bei einem Anwendungspartner nutzen wollen, verwenden Verimi zur sicheren Authentisierung gegenüber diesen. Die zur Nutzung des Services erforderlichen personenbezogenen Nutzerdaten werden von Verimi sicher an den Anwendungspartner übertragen. Dabei werden insbesondere drei Vorgaben beachtet:

- Anwendungspartner erhalten nur die für ihren Service benötigten Nutzer- oder Identitätsdaten (Zweckbindung), welche im Verimi-Profil der Nutzer hinterlegt sind
- Nutzer können individuell bestimmen, welche Daten an Anwendungspartner übermittelt werden (Transparenz sowie Durchsetzung des Rechts auf informationelle Selbstbestimmung)
- Nutzer werden über alle Datenübermittlungen informiert und können die Details der Transaktion mit Hilfe der Verimi Applikation einsehen.

Eine Datenverarbeitung außerhalb des oben beschriebenen Zwecks findet nicht statt. Verimi analysiert weder, welche Nutzer sich wann zu welchem Zweck bei welchen Anwendungspartnern anmelden,[3] noch werden diese Informationen an Dritte weitergegeben. Einzige Ausnahmen sind interne Datenanalysen zur Betrugsprävention oder aus regulatorisch-notwendigen Gründen.

2 Funktionen

Die zentralen Funktionen von Verimi umfassen aktuell erstens ein Identitätsmanagement, d.h. die Verwaltung der Daten und Berechtigungen im Zusammenhang digitaler Identitäten durch Nutzer mit Hilfe von Softwarelösungen, sowie die Möglichkeit die Datenschutzeinstellungen fallweise anzupassen Verimi bietet außerdem die Möglichkeit, mit einem einzigen Verfahren Zugang zu Online-servicen verschiedener Anwendungspartner zu erlangen, einen Zahlungsdienst, sowie die Möglichkeit Dokumente mittels einer QES (Qualifizierte Elektronische Signatur) online zu unterschreiben.

Die für diese Funktionen realisierten Sicherheitsmaßnahmen sind ebenso Basis für Funktionen weiterer Ausbaustufen, z.B. eID, qualifizierte elektronische Signatur oder die elektronische Bereitstellung von Funktionen deutscher oder europäischer Personaldokumente (Personalausweis, Pass, Aufenthaltstitel).

[3] Im Rahmen von Fraud Detection kann eine Analyse stattfinden, zudem werden anonymisierte Analysen durchgeführt und zur Verbesserung der Nutzererfahrung ausgewertet.

2.1 Identitätsmanagement[4]

Abhängig von den Services, die Nutzer über Verimi verwenden, werden verschiedene Identitätsattribute benötigt, z.B. Name, Vorname, Adresse, Geburtsdatum, aber auch Telefonnummern, E-Mail-Adressen und Bankverbindungen. Nutzer können individuell sowie frei entscheiden, welche ihrer Identitätsattribute sie über Verimi verwalten.

Wesentlich ist, dass die in Verimi verwendeten Daten authentisch sind, bei Änderungen aktualisiert werden können und nur die Inhaberinnen und Inhaber der Daten diese auch verwenden können. Aus diesem Grund legt Verimi größten Wert auf Sicherheit sowohl bei der Registrierung und Aktualisierung dieser Daten als auch bei ihrer Authentisierung.

2.1.1 Identifizierung von Nutzern

Nutzer haben mehrere Möglichkeiten, sich bei Verimi zu identifizieren:

- Über das Einlesen der Personalausweisdaten mittels der auf NFC basierenden eID Funktion
- Über das von der webID Solutions GmbH und der Identity Trust Management AG angebotene Verfahren Video-Ident
- Über Anwendungspartner, bei denen sich Nutzer bereits sicher registriert haben, z.B. die Deutsche Bank
- Über eine Identifikation am Point of Sale, inkl. Einlesen und Überprüfen des Personalausweises oder Reisepasses
- Über ein Bank-Ident-Verfahren gemäß der Zahlungsdienstrichtline PSD2

Hierbei werden die auf Personalausweis, Aufenthaltstitel bzw. Reisepass enthaltenen personenbezogenen Daten aufgenommen und sicher in Verimi gespeichert. Weitere personenbezogene Daten, die Nutzer über Verimi verwalten, müssen ebenfalls verifiziert werden. Die hierfür verwendeten Methoden sind abhängig von der Art der Daten. So werden z.B. Telefonnummern für mobile Endgeräte über eine SMS-Bestätigung und E-Mail-Adressen über eine E-Mail-Bestätigung verifiziert. Im ersten Fall erhalten Nutzer einen sechsstelligen Code an die angegebene Telefonnummer, der innerhalb der Verimi-Plattform bestätigt wird. Für die E-Mail-Verifikation wird ein Link via E-Mail versendet, der einen 16-stelligen Code enthält. Somit sind alle Identitätsattribute authentisch. Durch eine Verknüpfung der Daten mit passenden Authentifizierungsverfahren können die Identitätsattribute sicher gegenüber Anwendungspartnern sowohl zur Identifizierung als auch Authentifizierung verwendet werden.

2.1.2 Aktualisierung von Identitätsdaten

Identitätsdaten der Nutzer können sich mit der Zeit ändern, der Nachname bei Heirat, die Wohnadresse bei Umzug oder die Bankverbindung bei Wechsel der Bank.

In allen Fällen erfolgt die Aktualisierung der Identitätsattribute wie bei der Registrierung der Nutzer.

[4] Auf Basis des internationalen Standards ISO/IEC 29115 gibt in Europa die eIDAS (electronic Identification, Authentication and Trust Services) den regulatorischen Rahmen für Identitäts- und Vertrauensdienste vor. Daneben gelten in Deutschland eine Reihe weiterer gesetzlicher Bestimmungen, die Verfahren zur Identitätsfeststellung in speziellen Kontexten regeln, beispielsweise das Geldwäschegesetz (GwG), das Telekommunikationsgesetz (TKG), das Bundesmeldegesetz (BMG) oder das Carsharing-Gesetz (CsgG).

2.1.3 Account-Sperrung und -wiederaufnahme

Nutzer können ihren Verimi-Account über die Verimi-Plattform sperren: Nutzer melden sich bei Verimi mit einem der ihnen zur Verfügung stehenden Authentisierungsverfahren an und sperren ihren Account. Darüber hinaus wird der Account gesperrt, wenn das Passwort für das Authentisierungs-verfahren Benutzername/Passwort mehrmals falsch eingegeben wurde. Dabei wird zunächst nach fünf Fehlversuchen der Account für 30 Minuten gesperrt. Nach insgesamt 12 Fehlversuchen wird der Account für immer gesperrt.

In allen Fällen werden die Nutzer über die Sperrung ihres Accounts via E-Mail oder SMS benachrichtigt.

Um den Verimi-Account zu entsperren, melden sich Nutzer zunächst gegenüber Verimi mit einem ihrer Authentisierungsverfahren an. Verimi sendet ein One-Time-Passwort an die hinterlegte Mobilfunknummer oder E-Mail-Adresse, das zur Entsperrung des Accounts verwendet werden kann.

2.2 Anmeldung über Verimi

Über ihren Verimi-Account können sich Nutzer bei zahlreichen Anwendungspartnern anmelden. Hierfür werden kryptographische Protokolle genutzt, die sicherheitstechnisch sehr gut untersucht wurden und weltweit bereits vielfältig im Einsatz sind.

Anwendungspartner erhalten nur diejenigen Identitätsdaten, die sie für ihren Service benötigen. Beispielsweise erhalten Dienste, die Inhalte nur für volljährige Personen bereitstellen dürfen, auch nur genau diese Information. Online-Händler erhalten für die Bereitstellung ihres Dienstes die Identitätsattribute Name, Vorname, Adresse und Bankverbindung (und eventuell Informationen über das Alter).

Nutzer können aber zu jedem Zeitpunkt entscheiden, welche Identitätsdaten sie für welche Anwendungspartner zur Verfügung stellen wollen.

2.2.1 OpenID Connect

Die Anmeldung von Nutzern bei Anwendungspartnern über Verimi erfolgt über OpenID Connect als Erweiterung von OAuth2.0 im Authorization Code Flow. OpenID Connect ist ein Protokoll, das es ermöglicht, sich sicher über den zentralen Service Verimi bei verschiedenen Anwendungspartnern anzumelden, siehe auch [7]. Nutzer öffnen zunächst die Internetseite oder die App des Anwendungspartners und werden an Verimi weiterleitet. Hier melden sich die Nutzer mit einem ihrer Authentisierungsverfahren an. Für technische Details zu den bereitgestellten Token siehe Abschnitt 3.1.3.

2.2.2 Authentifizierung

Nutzer müssen sich gegenüber Verimi authentisieren, um sich bei beteiligten Anwendungspartnern anmelden zu können. Derzeit sind verschiedene Authentifizierungsverfahren umgesetzt:

- Benutzername/Passwort: Dieses Verfahren setzt eine Ein-Faktor-Authentifizierung um, die auf Wissen (das Passwort) basiert.
- Email-Link: Anstelle der Eingabe von Benutzername/Passwort erhält der Nutzer eine Email mit einem einmal verwendbaren Link an die zuvor verifizierte Email Adresse. Mit Aufrufen des Links ist der Nutzer erfolgreich authentifiziert und wird zur Seite des Anwendungspartners weitergeleitet.
- Verimi-App: Dieses Verfahren setzt eine Zwei-Faktor-Authentifizierung in einem einzigen Schritt um. Hierbei wird ein geheimer Schlüssel für ein asymmetrisches Challenge-Response-Verfahren in einem abgesicherten Bereich des Smartphones gespeichert (Faktor Besitz). Der geheime Schlüssel kann dabei nur zusammen mit einem weiteren Faktor verwendet werden, entweder dem Faktor Wissen (6-stelliger PIN) oder Biometrie (Fingerabdruck oder Gesichtserkennung).
- Die Ein-Faktor Authentifizierungsverfahren können mit der Verimi-App kombiniert werden, sodass sogar eine 3-Faktor-Authentifizierung zur Anwendung kommt.

Welches Verfahren zum Einsatz kommt, hängt von dem vom Anwendungspartner geforderten Sicherheitsniveau und den Wünschen des Nutzers ab. So ermöglicht die Anmeldung via Benutzername/Passwort die Nutzung von Services mit geringerem Sicherheitsniveau, dies könnten z.B. die Überweisung kleinerer Geldbeträge oder Bestellungen bei Online-Händlern sein. Mit einer Zwei-Faktor-Authentisierung könnten bspw. Bankkonten eröffnet, hohe Geldbeträge überwiesen und Versicherungsverträge abgeschlossen werden.

Die Sicherheitsexperten von Verimi entscheiden gemeinsam mit den beteiligten Anwendungspartnern, für welche Services welches Authentisierungsverfahren genutzt werden kann.

2.3 Qualifizierte elektronische Signatur (QES)

Nutzer, die sich auf der Verimi-Plattform identifiziert haben, können Dokumente digital und rechtswirksam unterschreiben. Bei dem von Verimi dafür bereitgestellten Unterschriftsservice handelt es sich um die Qualifizierte Elektronische Signatur (QES). Die QES ist die sicherste elektronische Signatur und erfüllt die Schriftformerfordernis.
Um diesen Service anzubieten arbeitet Verimi mit verschiedenen Vertrauensdienstleistern zusammen, u.a.. Infocert S.p.A. und Namirial S.p.A.. Unsere Partner sind entsprechend der eIDAS/IVT Verordnung europaweit zertifizierte Vertrauensdiensteanbieter für qualifizierte elektronische Signaturen.
Die Nutzer stimmen der sicheren Übertragung ihrer verifizierten Identitätsdaten von Verimi an den Vertrauensdienstleister und deren Speicherung zur Erstellung und Verwendung des Zertifikats mittels die Zwei-Faktor-Authentifizierung zu. Nach der Übermittlung der Identitätsdaten gehen die Nutzer einen Vertrag mit dem Vertrauensdiensteanbieter über das für die QES ausgestellte Zertifikat ein. Mit diesem Zertifikat erhalten sie die Möglichkeit, für die Dauer eines Jahres PDFs ihrer Wahl digital auf Verimi zu unterschreiben. Jede Unterschrift muss vom Nutzer mit der Zwei-Faktor-Authentifizierung freigeben werden.

2.4 Datenschutz

Verimi legt großen Wert auf Datenschutz. Alle Systeme wurden nach dem Prinzip „Privacy by Design" konzipiert, siehe auch [6].

2.4.1 Nutzer

Nutzer können jederzeit entscheiden, wem sie welche ihrer Identitätsattribute zur Verfügung stellen, und nachvollziehen, an welchen Anwendungspartner sie wann welche ihrer Identitätsattribute übertragen haben. Diese Differenzierung ermöglicht die Realisierung gestufter Opt-in-Verfahren, wie sie durch die Bestimmungen aus DSGVO und ePrivacy gefordert sind. Darüber hinaus wertet Verimi selbst die Aktivitäten der Nutzer nicht aus.[5] Alle diese Daten inklusive der Identitätsattribute sind, wie in Abschnitt 3.3.3 beschrieben, mit nutzerindividuellen Schlüsseln geschützt.

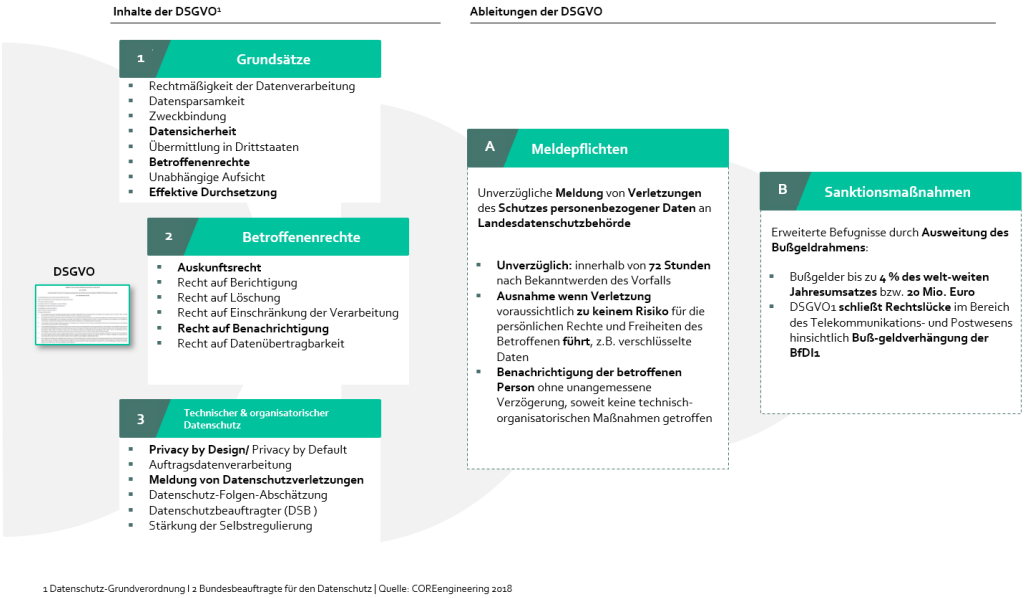


Abbildung 1: Übersicht Datenschutz-Grundverordnung

2.4.2 Anwendungspartner

Unterschiedliche Anwendungspartner erhalten verschiedene Identitätsattribute der Nutzer, um ihre Services umsetzen zu können. So benötigt z.B. ein Service, der nach Jugendschutzgesetz Inhalte online für Personen ab 16 oder 18 Jahren anbietet, lediglich die Information darüber, ob Nutzer das entsprechende Alter erreicht haben (aber nicht das genaue Geburtsdatum oder andere Identitätsdaten). Online-Händler, die ihre Waren an Kunden versenden, benötigen darüber hinaus auch die Identitätsattribute Name, Vorname, Adresse und eventuell Informationen über Bankverbindungen.

Bevor ein Anwendungspartner Verimi als Identity Provider nutzen kann, wird festgelegt, welche Identitätsattribute er für seinen Service erhält (Datensparsamkeit). Der Datenschutzbeauftragte von Verimi entscheidet gemeinsam mit den beteiligten Anwendungspartnern, welche Identitätsattribute diese für ihren Service von den Nutzern unbedingt benötigen. Weitere Daten werden den Anwendungspartnern nicht übermittelt.

Dabei richtet sich Verimi auch nach den Vorgaben der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und lässt sich von den zuständigen Landesdatenschützerinnen und -schützern beraten.

[5] Im Rahmen von Fraud Detection kann eine Analyse stattfinden, zudem werden anonymisierte Analysen durchgeführt und zur Verbesserung der Nutzererfahrung ausgewertet.

Die Information darüber, welche Anwendungspartner welche Identitätsattribute für ihren Service erhalten, wird bei jeder Übertragung angezeigt und muss bestätigt werden. So können Nutzer selbst entscheiden, ob sie diese Daten zur Verfügung stellen und den Service verwenden wollen (Opt-in).

3 Technologien

Alle Systeme von Verimi wurden von Anfang an in Hinblick auf die sichere Umsetzung des Service Verimi designed (Security by Design). Hierzu zählen nicht nur die verwendeten kryptographischen Verfahren, sondern auch die in diesem Abschnitt beschriebenen technischen infrastrukturellen, softwareseitigen und übergreifenden Elemente zur Absicherung der Plattform. Ablauf- und aufbauorganisatorische Elemente werden im folgenden Kapitel 4 beschrieben.

3.1 Infrastruktur/Plattform

Alle von Verimi verwalteten Daten der Nutzer sind zu jeder Zeit geschützt, innerhalb der Verimi-Plattform, auf dem Übertragungsweg und beim Anwendungspartner. Für den Schutz der Identitätsdaten werden nur kryptographische Verfahren eingesetzt, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen werden. Dabei werden die vom BSI veröffentlichten Technischen Richtlinien [3] und [4] beachtet. Darüber hinaus sind die in Verimi eingesetzten kryptographischen Verfahren in einem Kryptokonzept beschrieben, das nach Vorgaben des BSI (siehe [5]) erarbeitet wurde.

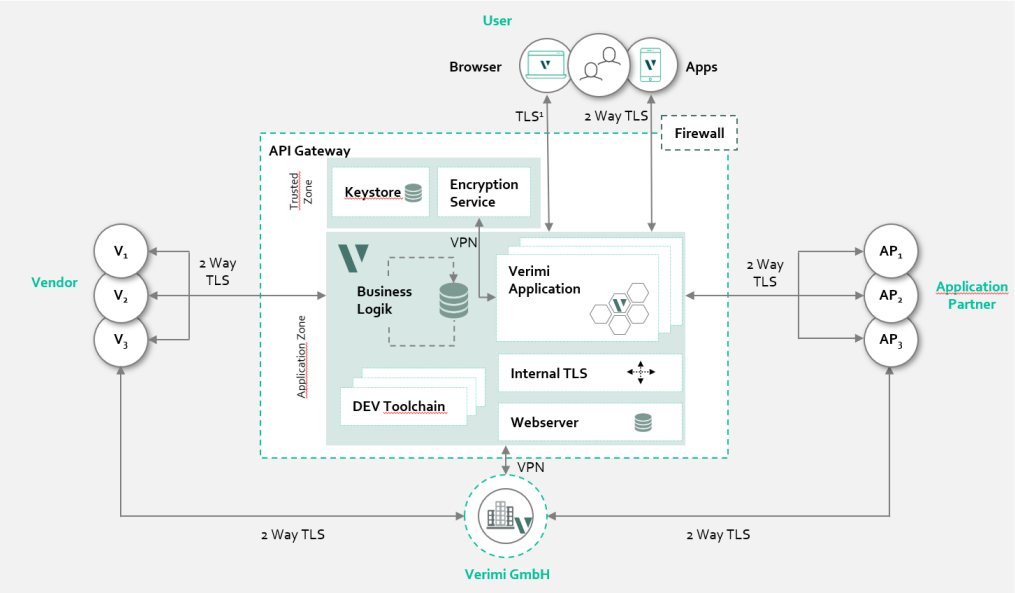


Abbildung 2: Überblick Sicherheitsarchitektur Verimi

Sollten sich in der Zukunft Sicherheitslücken bei Einsatz findenden kryptographischen Verfahren ergeben, ist der umgehende Wechsel auf andere Verfahren sicherzustellen. Hierfür existiert ein Migrationskonzept, mit Hilfe dessen zeitnah auf alternative Verfahren umgeschwenkt werden könnte.

3.1.1 Speicherung/Löschung

Verimi verwaltet die von Nutzern im Rahmen der Registrierung übermittelten Identitätsattribute. Zu diesen gehören Name, Vorname, Adresse, Geburtsdatum, Geburtsort, Telefonnummer(n), E-Mail-Adresse(n) und Bankverbindung(en). Verimi generiert und speichert darüber hinaus weitere

Identitätsattribute: Eine UUID[6] , um Nutzer eindeutig innerhalb von Verimi zuordnen zu können, mehrere eUUIDs[7] , um Nutzer eindeutig innerhalb der Anwendungspartner zuordnen zu können und, abhängig vom genutzten Authentisierungsverfahren, die E-Mail-Adresse (bei Nutzung des Verfahrens Benutzername/Passwort), bzw. den öffentlichen Schlüssel bei Nutzung der Zwei-Faktor-Authentisierung über die Verimi-App.

UUID, öffentlicher Schlüssel sowie die verschlüsselte E-Mail-Adresse bilden die sogenannte Verimi-ID, die innerhalb von Verimi genutzt wird.

Darüber hinaus werden alle Transaktionen, die Nutzer über Verimi bei Anwendungspartnern durchführen, ebenfalls in Verimi solange gespeichert wie der Account besteht, damit Nutzer zu jeder Zeit nachvollziehen können, welchem Anwendungspartner sie wann zu welchem Zweck welche ihrer Identitätsattribute zur Verfügung gestellt haben.

Mit Blick auf die Löschung können Nutzer ihren Account entweder unmittelbar, d.h. sofort zur Löschung freigeben oder zunächst nur blockieren. Sofern die Nutzer nach der Blockierung keine weiteren Aktivitäten nachweisen, wird der Account nach sechs Monaten automatisch gelöscht. Während der sechsmonatigen Karenzzeit besteht die Möglichkeit, den Account zu reaktivieren und Verimi erneut zu nutzen. Weitere Einzelheiten können Verimis Datenschutzerklärung entnommen werden.

Mit der Löschung wird das Schlüsselmaterial gelöscht; auch die nutzerindividuellen Attribute werden in diesem Fall unwiederbringlich gelöscht.

3.1.2 Kommunikation

Alle Kommunikationswege werden mittels Transport Layer Security (TLS 1.2) gesichert. Diese sind:

- Kommunikationsweg zwischen Nutzerin/Nutzer und Anwendungspartner
- Kommunikationsweg zwischen Nutzerin/Nutzer und Verimi
- Kommunikationsweg zwischen Verimi und Anwendungspartner

Alle Daten werden also sowohl verschlüsselt als auch authentisiert übertragen. Zum Einsatz kommen ausschließlich Cipher Suites, die vom BSI in [4] empfohlen sind.

Die jeweiligen Kommunikationspartner müssen sich im Rahmen des Aufbaus der TLS-Verbindung authentisieren. Zwischen Verimi und Anwendungspartner werden X.509-Zertifikate genutzt, die von vertrauenswürdigen Certification Authorities (CA) ausgestellt wurden. Verimi akzeptiert nur Zertifikate der folgenden CAs:

[6] UUID ist die Abkürzung für Universally Unique Identifier.
[7] eUUID ist die Abkürzung für external Universally Unique Identifier. Dabei erhält jeder Anwendungspartner eine spezifische UUID, um ein Tracking von Nutzerverhalten Service- oder Partner-übergreifend über Verimi zu verhindern.

- GlobalSign, https://www.globalsign.com
- thawte, https://www.thawte.de
- digicert, https://www.digicert.com
- D-Trust, https://www.d-trust.de

Nutzer authentisieren sich gegenüber Verimi mit einem der in Abschnitt 2.2.2 beschriebenen Authentisierungsverfahren.

Die Kommunikation zwischen der Verimi GmbH und der Verimi-Plattform erfolgt über eine VPN-gesicherte Verbindung.

3.1.3 Zugriff

OpenID Connect

Die Anmeldung der Nutzer bei Anwendungspartnern erfolgt mittels OpenID Connect. Nach erfolgreicher Authentifizierung der Nutzer stellt Verimi zwei Token für den Anwendungspartner bereit, die jeweils einen singulären Zweck erfüllen:

- ID-Token enthalten eine eindeutige Kennung, durch die der Anwendungspartner Nutzer in seinem System identifiziert. Um ein Tracking zu unterbinden, erhalten Anwendungspartner individuelle Kennungen.
- Access-Token gewähren Zugriff auf die Inhalte der freigegebenen Datengruppen. Sie haben eine Gültigkeit von 60 Sekunden und müssen bei jeder lesenden oder schreibenden Anfrage an die Verimi-Plattform übermittelt werden.

Die Aushändigung der Token geschieht nach gegenseitiger Authentisierung zwischen Anwendungspartner und der Verimi-Plattform (siehe Abschnitt 3.1.2) im Austausch gegen den Authorization Code. Dieser wird dem Anwendungspartner über die Nutzer nach erfolgreicher Anmeldung auf der Verimi-Plattform ausgehändigt. Der Authorization Code ist eine NONCE[8] aus dem Alphabet {0,…, 9,a,…,z,A,…,Z,-, _} der Länge 16 mit Gültigkeit von 60 Sekunden. Damit ist sichergestellt, dass Anwendungspartner nur dann auf die Identitätsattribute der Nutzer zugreifen können, wenn diese dies freigegeben haben.

ID- und Access-Token sind JSON Web Token (JWT), siehe [1], deren Header und Payload signiert sind. Zur Erstellung der Signatur wird der Signaturalgorithmus ECDSA-SHA384 (Kurve P-384, siehe [8]) genutzt. Die jeweiligen Payloads enthalten neben den oben beschriebenen Inhalten und dem Zeitpunkt der Erstellung zusätzlich eine NONCE ebenfalls aus dem Alphabet {0,…, 9,a,…, z, A,…, Z, -, _} der Länge 16. Mit der Signatur bestätigt Verimi, dass sich die Nutzer gegenüber Verimi authentisiert haben und die übermittelten Identitätsattribute authentisch sind.

Alle benötigten Zufallswerte (Schlüsselpaare für die Signatur, Zufallswerte zu Erzeugung der Signaturen, NONCEs für Authorization Code, ID- und Access-Token) werden mit dem in Abschnitt 3.3.3 beschriebenen Zufallszahlengenerator erzeugt.

[8] NONCE bedeutet Number Only Used Once

Die OpenID Connect Umsetzung von Verimi ist seit dem Release 1.2 von der OpenID Foundation zertifiziert: https://openid.net/certification/

Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung (2FA) der Verimi-Apps nutzt die Faktoren Besitz und Wissen oder die Faktoren Besitz und Sein. Im ersten Fall liegt der Schlüssel als Faktor Besitz im gesicherten Bereich des Smartphones, zu dem der Zugang über die PIN gewährt wird. Im zweiten Fall wird der Zugang zum Schlüssel über den Fingerabdruck, oder die Gesichtserkennung gewährt.

3.2 Software/Anwendungen

3.2.1 Verimi Web-Anwendung und Mobile Apps

Die Verimi-Plattform besteht aus drei Kernanwendungen, die jeweils vollumfängliche Funktionalität bieten:

- der Web-Anwendung, die über das Internet erreichbar ist und über beliebige Browser genutzt werden kann
- der nativen iOS-App für ein optimiertes Nutzererlebnis auf Apple-Geräten
- der nativen Android-App für ein optimiertes Nutzererlebnis auf Geräten mit Android-Betriebssystem

Die Anwendungen werden kontinuierlich weiterentwickelt. Neben den Tests auf mögliche Sicherheitslücken werden die Security-Verbesserungen der jeweiligen Betriebssysteme integriert.

3.2.2 Härtungen

Das Betriebssystem der Plattform ist ein Linux-Derivat, bei dem sämtliche nicht benötigten Funktionen deaktiviert sind sowie alle sicherheitserhöhenden Features eingeschaltet sind. Dies umfasst insbesondere die Konfigurationsgruppen Dateisystem, Software-Updates und Integritäts-Checks.

Auch die Verimi-Apps für Android und iOS sind mit Hilfe eines Tools gehärtet: Das Trusted Application Kit (TAK) der Firma Build38 (Ausgründung von Giesecke+Devrient) verfügt u.a. über White Box Crypto zur Obfuskation von Schlüsseln und Kryptofunktionen, 2 Way TLS, sicheren Speicher, Hook und Root Detection sowie Device Fingerprinting zur Bindung an das Smartphone.

3.2.3 CQRS – Command-Query-Responsibility-Segregation

In der CQRS-Architektur sind die Komponenten Kommando (Writer) und Query (Reader) voneinander getrennt. Dies ermöglicht die Erstellung eines unabhängigen Schreib- und Abfragemodells, um spezifischen Bedürfnissen des Systems zu entsprechen. So kann beispielsweise die Betrugserkennungskomponente bei jedem ungültigen Anmeldeversuch einen Eintrag in der Datenbank erstellen, während die Betrugsabfragekomponente ein aggregiertes Modell mit einer entsprechenden Ansicht dieser ungültigen Anmeldeversuche liefert.

Darüber hinaus ist die CQRS-Architektur für Anwendungen von Vorteil, bei denen das typische Nutzungsmuster zwischen Schreiben und Lesen nicht gleichmäßig verteilt ist. CQRS erlaubt, bei leseintensiven Anwendungen mehr Leseinstanzen zu starten, während zeitgleich nur eine Befehlskomponente angesteuert wird, um die Last zu tragen.

3.3 Übergreifende technische Elemente

3.3.1 Physische Sicherheit

Alle für die Umsetzung des Services Verimi benötigten IT-Komponenten (Server, Datenbanken) sind in speziell abgesicherten Lokationen untergebracht. Zugang zu den Räumlichkeiten haben nur Administratorinnen und Administratoren unter Wahrung des Vier-Augen-Prinzips, d.h. es müssen sich zwei Personen mittels personalisierter Chipkarten und PIN gegenüber den gesicherten Zugängen authentisieren, um Zutritt zu erhalten. Jeder Zutritt wird revisionssicher protokolliert und regelmäßig vom Sicherheitsteam der Verimi analysiert.

Die Lokationen sind weitreichend gesichert. Zudem sind sie mit mehrstufigen Alarmanlagen ausgestattet, sodass Einbrüche zu jeder Zeit erkannt und an das zuständige Sicherheitsteam weitergeleitet werden.

Ergänzend wird ein Zwei-Zonen-Modell umgesetzt. Server und Datenbanken für den sicheren Betrieb von Verimi sind in Application Zone untergebracht. Services für das Schlüsselmanagement (Zufallszahlengenerator, Speicherung der nutzerindividuellen Schlüssel zur Verschlüsselung der Identitätsattribute) in der Trusted Zone. Der Zugriff auf diese IT-Komponenten ist noch einmal zusätzlich durch eine 3 Faktor Authentifizierung (inkl. einer FIPS 140-2 zertifizierten Yubikey Hardware) geschützt. Die Trusted Zone ist mittels eigener Virenscanner, Firewalls und Intrusion Detection-/Intrusion Prevention-Systeme abgesichert und wird separat von der Application Zone geloggt und analysiert.

3.3.2 PKI – Public-Key-Infrastruktur

Für Netzwerkverbindungen auf der Verimi-Plattform ist eine starke Authentifizierung auf Basis digitaler Zertifikate erforderlich. Dies umfasst die Authentisierung der Verimi-internen Kommunikation von Services, der externen Kommunikation mit Anwendungspartnern und des Zugriffs von Administratorinnen und Administratoren auf das Log- und Monitoring-System. Die technische Plattform basiert auf den X.509 ITU-T-Standard für die Public Key Infrastructure (PKI).

Zur Absicherung der Verimi Plattform werden multiple Instanzen (Certificate Authorities) über eine hierarchische PKI zur Ausgabe von selbst-signierten Zertifikaten eingesetzt. Als Stammzertifizierungsinstanz wird die Verimi Root Certificate Authority (Root-CA) verwendet.

3.3.3 Verschlüsselung

Datenverschlüsselung

Identitätsattribute und Transaktionsdaten werden verschlüsselt und authentisch (d.h. gegen Manipulation gesichert) zusammen mit der Verimi-ID in Datenbanken gespeichert. Hierzu werden für alle Nutzer individuelle Schlüssel erzeugt. Für die Verschlüsselung und Authentisierung wird das Verfahren AES im Cipher Block Chaining Mode eingesetzt.

Für die Erstellung neuer individueller Schlüssel und für deren Verwendung, um persönliche Daten zu ver- und entschlüsseln wird ein separater Service innerhalb der Trusted Zone verwendet. Dur Zugriff zur Trusted Zone (z.B. um den Service zu starten oder zu konfigurieren) ist nur vertrauenswürden Mitarbeitern von Verimi möglich, die in Besitz des Master Schlüssel sind. In der Trusted Zone existiert

der System Schlüssel, der verwendet wird, um individuelle Schlüssel zu ver- und entschlüsseln. Weder der System Schlüssel noch die Individuellen Schlüssel können aus der Trusted Zone ausgelesen werden. Stattdessen bietet diese eine geschützte Schnittstelle, die es ermöglicht Benutzerdaten passend für den jeweiligen Nutzer zu ver- oder entschlüsseln.

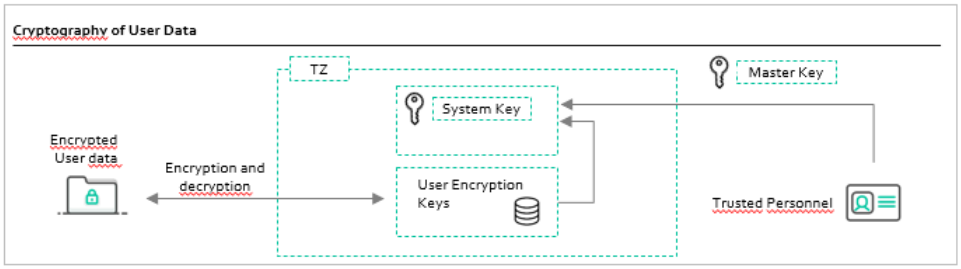


Abbildung 3: Überblick Methoden für Generierung und Verwendung kryptographischer Schlüssel

Melden sich Nutzer bei Verimi an, wird zunächst die UUID bestimmt. Für das Verfahren Benutzername/Passwort wird der Benutzername (eine E-Mail-Adresse) in der Datenbank gesucht und damit die UUID extrahiert. Bei Nutzung der Zwei-Faktor-Authentisierung der Verimi-Apps wird der öffentliche Schlüssel der Verimi-App genutzt, um die UUID zu ermitteln.

Anhand der UUID werden die verschlüsselten Identitätsattribute, die der Anwendungspartner für seinen Service benötigt, identifiziert und diesem zur Verfügung gestellt, die eUUID über das ID-Token, die weiteren Attribute nach Vorlage des Access-Token.

Die Passwörter der Nutzer werden nicht im Klartext innerhalb von Verimi gespeichert, sondern es wird zusammen mit einem Zufallswert (einem sogenannten Salt) und der Funktion bcrypt ein Hash erzeugt und zusammen mit dem Salt gesichert.

Alle eingesetzten Schlüssel haben eine Länge von 256 Bit und sicher in der Trusted Zone gespeichert. Zugriff zur Trusted Zone ist nur mittels einer 3-Faktor-Authentifizierung incl. Besitzes eines FIPS 140-2 zertifizierten Hardware Tokens möglich.

Zufallszahlengeneratoren

Die Sicherheit der genutzten kryptographischen Verfahren und Protokolle hängt maßgeblich von der Entropie (von der Unvorhersagbarkeit) der eingesetzten Schlüssel und der verwendeten kryptographischen Parameter ab. Verimi nutzt zur Erzeugung dieser Werte Zufallszahlengeneratoren, die von offiziellen Stellen, z.B. dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem National Institute of Standards and Technology (NIST) für den Einsatz in hochsensiblen Bereichen empfohlen werden.

Für die Erzeugung der benötigten Zufallswerte wird der deterministische Zufallszahlengenerator /dev/urandom des zugrunde liegenden Linx Systems verwendet.

3.3.4 Cloud Infrastruktur

Verimi nutzt die Open Telekom Cloud (OTC), eine Public Cloud auf Basis von Openstack. Die OTC ist eine Infrastructure-as-a-Service-(IaaS-)-Lösung, die den Zugriff auf virtuelle IT-Infrastrukturen über das

Internet ermöglicht. Innerhalb des OTC-Virtual Datacenter verwendet Verimi folgende Funktionen selbständig:

- Einrichten und Verwalten von
    - ECS (Elastic Cloud Server) Instanzen
    - Dedizierte Server mit virtuellem Hypervisor
    - Bare Metal Server ohne unmittelbare Virtualisierung
- Verwalten von Netzwerkkomponenten (VPCs, Netzwerke, Subnetzwerke, Firewalls, Netzwerksicherheitsgruppen und NAT Gateways
- Einrichtung und Durchführung von Sicherungskopien
- Überwachung der Komponenten des Rechenzentrums mittels Cloud Trace Monitorings

3.3.5 Intrusion Detection und Prevention

Verimi nutzt Virenscanner und Firewalls verschiedener Anbieter, um sich vor Angriffen von außen zu schützen. Virensignaturen und Firewall-Konfigurationen werden regelmäßig aktualisiert und an die aktuelle Sicherheitslage angepasst.

Diese Maßnahmen allein reichen nicht aus, um die Plattform zu schützen. So werden z.B. sogenannte Zero Day Exploits (Sicherheitslücken, die bisher nicht bekannt waren) hierdurch nicht erkannt. Um auch auf aktuelle Angriffe reagieren zu können, wurden innerhalb der Verimi-Plattform verschiedene Intrusion Detection- und Intrusion Prevention-Systeme implementiert, die Angriffe durch Anomalieerkennung detektieren und entsprechende Gegenmaßnahmen einleiten können.

Zusätzlich werden alle Aktivitäten erfasst, gespeichert und regelmäßig von den Sicherheitsexperten mit Hilfe etablierter Tools hinsichtlich Auffälligkeiten untersucht, sodass auch eine manuelle Überprüfung der Sicherheit des Systems gewährleistet ist.

3.3.6 ISMS – Informations-Sicherheits-Management-System

Verimis Informationssicherheits-Managementsystem ist nach ISO 27001 zertifiziert. Zusätzlich zum ISMS werden auch ein Datenschutz-Management-System (DMS) sowie ein Compliance-Management-System (CMS) umgesetzt.

4 Organisation

Neben dem Einsatz technischer Maßnahmen zur Absicherung der Daten müssen auch organisatorische und personelle Maßnahmen für den sicheren Betrieb von Verimi umgesetzt werden.

Die notwendigen Sicherheitsmaßnahmen werden nicht nur von kompetenten Mitarbeiterinnen und Mitarbeitern mit Unterstützung renommierter Forschungseinrichtungen entwickelt und umgesetzt, sondern auch extern auf Vollständigkeit und Wirksamkeit evaluiert, siehe hierzu Anhang A.

Die Erarbeitung der Sicherheitsmaßnahmen erfolgt nach etablierten Vorgehensmodellen. Hierzu gehören, neben der Umsetzung aktueller Sicherheitsmaßnahmen, auch Aktivitäten zur Aufrechterhaltung im laufenden Betrieb (z.B. Notfallmanagement, Vorgehen bei Sicherheitsvorfällen und Anpassungen der Maßnahmen hinsichtlich der aktuellen Sicherheitslage).

4.1 Aufstellung

4.1.1 Sicherheitsteam

Das Sicherheitsteam besteht aus einem Informationssicherheitsbeauftragten und mehreren Sicherheitsexpertinnen und -experten.

Aufgaben des Sicherheitsteams sind, neben der Erarbeitung personeller, organisatorischer, technischer und infrastruktureller Sicherheitsmaßnahmen, auch die Umsetzung dieser Maßnahmen und die Aufrechterhaltung im laufenden Betrieb. Hierfür müssen nicht nur alle Mitarbeiterinnen und Mitarbeiter der Verimi regelmäßig geschult, sondern auch Anpassungen an die aktuelle Sicherheitslage vorgenommen werden, um auf eventuell auftretende Sicherheitsvorfälle reagieren zu können.

Die Sicherheit von Verimi wird laufend überprüft und verbessert, basierend auf dem vom OWASP entwickelten „DevSecOps Maturity Model" (DSOMM). Dabei unterstützen renommierte Forschungseinrichtungen, z.B. das Fraunhofer-Institut AISEC und die Arbeitsgruppe Identitätsmanagement der Freien Universität Berlin in den Jahren 2018-2020.

4.1.2 Zuverlässigkeitsüberprüfungen

Alle Mitarbeiterinnen und Mitarbeiter von Verimi werden vor Einstellung hinsichtlich ihrer Qualifikation für die von ihnen verantworteten Aufgaben eingehend überprüft. Dabei werden Ausbildung und vorhergehende Anstellungen an Hand von Ausbildungs- und Arbeitszeugnissen geprüft. Darüber hinaus müssen alle zukünftigen Mitarbeiterinnen und Mitarbeiter ein polizeiliches Führungszeugnis vorlegen.

4.1.3 Sicherheitsschulungen

Verimi führt regelmäßig Sicherheitsschulungen durch, um für das Thema IT-Sicherheit und Datenschutz zu sensibilisieren. Schulungen sind nicht nur für das technische Personal von Verimi (z.B. Systemadministratorinnen und Entwicklerinnen) verpflichtend, sondern auch für die Mitarbeiterinnen und Mitarbeiter der Verwaltung und an die jeweiligen Zielgruppen angepasst. In den Schulungen werden alle relevanten Themen der IT-Sicherheit und des Datenschutzes, von aktuellen Bedrohungen über Vorgehen von Angreiferinnen und Angreifern (auch Social Engineering) bis hin zu Folgen erfolgreicher Angriffe und Methoden zur Risikominimierung behandelt.

Darüber hinaus sind im Rahmen der regelmäßig stattfindenden Verimi Days renommierte Forscherinnen und Forscher eingeladen, über aktuelle Themen aus ihren Arbeiten vorzutragen und deren Ergebnisse zu diskutieren. Der Einblick in innovative Technologien erlaubt die laufende Verbesserung von Verimi.

4.1.4 Sicherheitsrelevante Rollen

Datenschutzbeauftragter

Konform zur neuen Datenschutz-Grundverordnung der Europäischen Kommission hat Verimi einen Datenschutzbeauftragten bestellt. Der Datenschutzbeauftragte wird nicht nur von einem Team aus qualifizierten Mitarbeiterinnen und Mitarbeitern unterstützt, sondern auch von renommierten wissenschaftlichen Einrichtungen. Hinsichtlich Datensicherheit arbeitet das Datenschutzteam eng mit dem Sicherheitsteam von Verimi zusammen.

Informationssicherheitsbeauftragter

Verimi hat einen Informationssicherheitsbeauftragten (ISB) bestellt. Zu seinen wesentlichen Aufgaben gehören

- Abstimmung von Informationssicherheitszielen mit der Unternehmensleitung
- Koordinierung und Planung der Informationssicherheit in Kooperation mit dem Informationssicherheitsteam (IST)
- Erstellung und Pflege von Richtlinien und Regelungen zur Informationssicherheit im Unternehmen
- Beratung der Unternehmensleitung in Fragen der Informationssicherheit
- Dokumentation von Informationssicherheitsmaßnahmen
- Schulung von Beschäftigten bzgl. Informationssicherheit
- Planung und Konzeption des Managements von Vorfällen („Incidents") sowie der Notfallvorsorge (inkl. Notfallplan/-handbuch)

Compliance-Beauftragter

Verimi hat einen Compliance-Beauftragten (CSB) bestellt. Der CSB implementiert die Compliance-Regelungen der Verimi in die Unternehmensstruktur und die Geschäftsprozesse durch den Aufbau eines Compliance-Managementsystems. Mit seinen Kenntnissen über die Unternehmensstruktur sowie die betrieblichen Prozesse und Produkte ermittelt er die unternehmensspezifischen Risiken für Rechtsverstöße in einer systematischen Risikoanalyse.

4.2 Prozesse

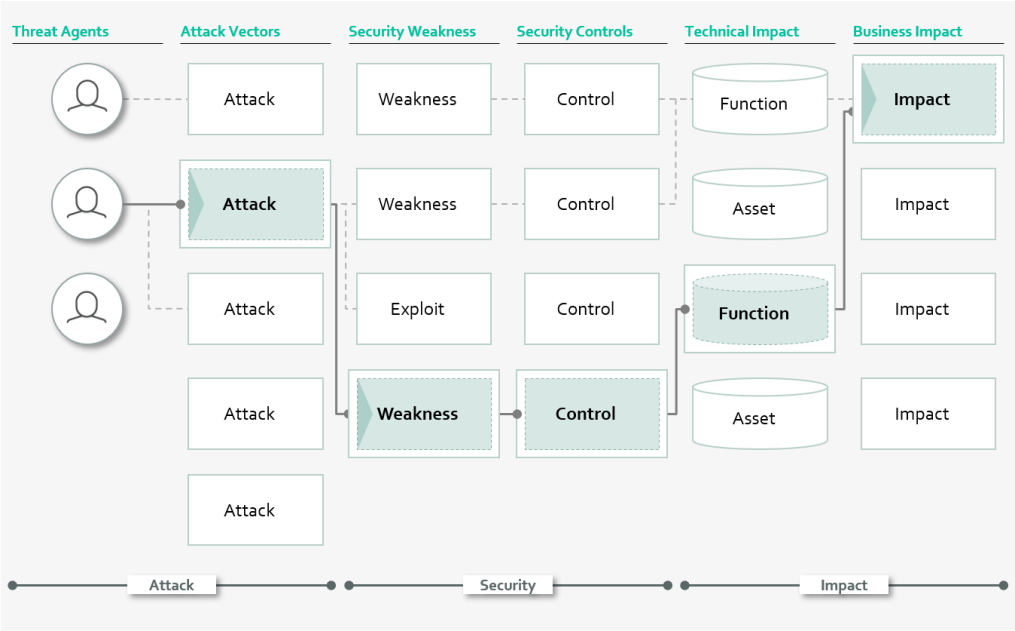
4.2.1 Softwarequalität in der Entwicklung

Bei der Entwicklung der Software für die Umsetzung des Services Verimi liegt der Fokus auf der Qualität der Software, um Sicherheitslücken, die sich aus Softwarefehlern ergeben, zu minimieren. Die Software muss vor Einsatz in das bestehende System mehrere Qualitätssicherungstests durchlaufen.

Ein Schwerpunkt liegt auf der Verhinderung von bekannten Angriffen, zum Beispiel den OWASP Top-Zusammenstellungen.

Da selbst mit intensiven Tests und klaren Spezifikationen Fehler nicht vollständig ausgeschlossen werden können, werden regelmäßig Penetrationstests durchgeführt, um Sicherheitslücken frühzeitig erkennen und beheben zu können.

Zur Steuerung der Pentests wird ein etabliertes Modell verwendet, das auf der Analyse der Höhe der Risiken (aus Wahrscheinlichkeit und Umfang der technischen und Business-seitigen Auswirkungen) aufsetzt. Zur Durchführung der Pentests werden sowohl interne als auch externe Ressourcen genutzt.



Quelle: OWASP 2018

Abbildung 4: Modell für Risikobewertung Angriffsvektoren, siehe [10]

4.2.2 Schwachstellenmanagement

Software kann Fehler haben. Einige dieser Fehler können zu Sicherheitslücken führen. Gleiches gilt für die umgesetzten Sicherheitsmaßnahmen, seien sie personeller, organisatorischer, technischer oder infrastruktureller Natur. Trotz Evaluierung dieser Maßnahmen hinsichtlich Sicherheit können sich Sicherheitslücken ergeben, die im Rahmen der Evaluierung nicht erkannt wurden.

Das Sicherheitsteam prüft daher regelmäßig die Wirksamkeit der umgesetzten Maßnahmen, auch durch Simulation eigener Angriffe (Hacking, aber auch z.B. Phishing-Angriffe), und testet so die Wirksamkeit der Sicherheitsmaßnahmen und Sicherheitsschulungen.

4.2.3 Vorgehen bei Sicherheitsvorfällen

Sollten sich Sicherheitslücken zeigen, z.B. durch eigene Beobachtungen oder aus tatsächlichen Angriffen, hat das Sicherheitsteam bereits mögliche Angriffsszenarien durchgespielt und entsprechende Gegenmaßnahmen vorbereitet. Diese können von kurzfristiger Abschaltung sicherheitskritischer Dienste bis hin zur Abschaltung der gesamten Plattform reichen, bis die Sicherheit wiederhergestellt ist.

Darüber hinaus wird regelmäßig die aktuelle Sicherheitslage beobachtet. Weitere Quellen, z.B. das Computer Emergency Response Team des Bundesamtes für Sicherheit in der Informationstechnik und

die Plattform Common Vulnerabilities and Exposures (CVE®), liefern Informationen über aktuelle Sicherheitslücken und Angriffe, um entsprechende Gegenmaßnahmen einzuleiten.

4.2.4 Evaluierung und Zertifizierung

Alle Bestandteile der Verimi-Infrastruktur werden nach etablierten Vorgehensmodellen evaluiert und zertifiziert. Dabei wird sowohl überprüft, ob für alle Sicherheitsrisiken entsprechende Sicherheitsmaßnahmen umgesetzt sind, als auch, wie wirksam diese Maßnahmen sind (d.h. ob sie die Risiken geeignet minimieren). Dies betrifft nicht nur den aktuellen Stand der Umsetzung, sondern auch, ob geeignet auf Sicherheitsvorfälle oder aktuelle Entwicklungen hinsichtlich Angriffen reagiert werden kann.

Verimi-Apps

Die Verimi-Apps sind eine Software für Smartphones, mit dem sich Nutzer sowohl mit Benutzername/Passwort als auch mit einer Zwei-Faktor-Authentisierung gegenüber Verimi (und damit über OpenID Connect auch gegenüber Anwendungspartnern, siehe Abschnitt 2.2.1) sicher authentisieren können.

Verimi GmbH und Plattform

Verimis Informationssicherheits-Managementsystem ist seit 2019 nach ISO 27001 zertifiziert. Diese Zertifizierung wird regelmäßig erneuert. Unser Informations Sicherheits Management System umfasst die gesamte Plattform, die Verimi Apps, die verwendete Hosting Infrastruktur, ebenso wie unsere Arbeitsmittel (IT, Prozesse und die Verimi Organisation).

4.2.5 BCM – Business Continuity Management

Das Business Continuity Management (BCM) schützt Verimi im Notfall vor ernsthaften Schädigungen oder existenzgefährdenden Verlusten. Es gilt über Verimi hinaus auch für externe Dienstleister. Es beschreibt inhaltliche, personelle und organisatorische Festlegungen und Verfahren für das Notfallmanagement, um

- bei Eintritt eines Notfalls die Fortführung der zeitkritischen Aktivitäten und Prozesse zu gewährleisten
- mit angemessenen Maßnahmen Schadenseintritte möglichst zu vermeiden
- die Auswirkungen eingetretener Schäden zu reduzieren
- eine schnelle und geordnete Wiederherstellung des Normalbetriebs zu unterstützen

Der Notfallverantwortliche für Verimi ist benannt, die Definition der Begriffe sowie der Prozesse nach Plan – Do – Check – Act erfolgt. Das Notfallhandbuch beschreibt die Notfallstrategien unter Berücksichtigung definierter Notfallszenarien und deren Kritikalität. Festlegungen und Details sind in der Richtlinie „Business Continuity Management" beschrieben.

5 Schluss

Sicherheit im digitalen Raum ist eines der aktuell drängendsten Themen. Verimi liefert hierzu einen Beitrag in dreifacher Weise:

- Als Service bietet Verimi eine sichere Identitätsmanagement-Plattform, mit der Nutzer ihre digitale Identität sicher verwalten und Anwendungspartner auf sichere digitale Identitäten zugreifen können
- In der Produktion im Sinne der inneren Konstruktion greift Verimi auf sichere Technologien und Best current practices zurück nach Maßgabe ständiger Weiterentwicklung und Verbesserung
- In der gesellschaftlichen Dimension schließlich kann Verimi als Instrument der Emanzipation fungieren, indem es Nutzern die Hoheit und Kontrolle über ihre personenbezogenen Daten verschafft

Die Diskussion dieser Dimensionen ist in hohem Maße notwendig. Da die Dimensionen sowohl für sich als auch insgesamt durch eine signifikante Dynamik gekennzeichnet sind, sind neben den permanenten Anpassungen der technologischen Ebene auch Gesichtspunkte hinsichtlich Funktionalität und gesellschaftlicher Entwicklung von Bedeutung. Der Diskurs ist unter wirtschaftlicher, staatlich-politischer, zivilgesellschaftlicher und technologischer Beteiligung zu führen – vor dem Horizont eines Interessenausgleichs dieser Gruppen.

Anhang

A. Begleitung

Verimi wird ständig weiterentwickelt und hinsichtlich Sicherheit untersucht. Dabei unterstützen zwei Forschungseinrichtungen, die Arbeitsgruppe Identitätsmanagement an der Freien Universität Berlin unter Leitung von Prof. Dr. Marian Margraf und das Fraunhofer Institut für Angewandte und Integrierte Sicherheit (AISEC) unter Leitung von Prof. Dr. Claudia Eckert in den Jahren 2018-2020, sowie COREengineering als Entwicklungspartner für Konzeption und Operationalisierung der Sicherheitsfunktionen.

B. Glossar

Identifikation (=Identifizierung)	Behauptung sowie Nachweis, eine bestimmte Person mit Name, Geburtsdatum, Geburtsort etc. zu sein (i.e.S.: Personenstammdaten, hoheitliche Ausweise; i.w.S.: Ansprüche wie Familie, Eigentumstitel, Beruf usw.)
Authentifizierung (=Authentifikation)	Überprüfung der digitalen Identität einer Person durch eine dazu berechtigte Instanz anhand verschiedener Mittel in den Kategorien Sein, Wissen, Besitz
Authentisierung (=Authentikation)	Elektronischer Nachweis der Identität einer Person durch diese Person selbst anhand von geeigneten Nachweismitteln in den Kategorien Sein, Wissen, Besitz
Autorisierung	Ermächtigung einer Aktion durch eine dazu berechtigte Person, ggf. auch Ermächtigung einer weiteren Person zur Durchführung der Aktion

C. Literatur

[1] T. Bray: The JavaScript Object Notation (JSON) Data Interchange Format, Request for Comments (RFC): 7159.

[2] BSI: IT-Grundschutzkataloge, Bundesamt für Sicherheit in der Informationstechnik.

[3] BSI: TR 02102-1, Kryptographische Verfahren: Empfehlungen und Schiüssellängen, Version 2016-01, 15. Februar 2016, Bundesamt für Sicherheit in der Informationstechnik.

[4] BSI: TR 02102-2, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS), Version 2016-01, Bundesamt für Sicherheit in der Informationstechnik.

[5] BSI: Leitfaden, Erstellung von Kryptokonzepten, Version 1.0, 2008, Bundesamt für Sicherheit in der Informationstechnik.

[6] A. Cavoukian: Privacy by Design: The 7 Foundational Principles, https://www.ipc. on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

[7] D. Hardt: The OAuth 2.0 Authorization Framework, Internet Engineering Task Force (IETF), Request for Comments (RFC): 6749.

[8] NIST: Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 01/2012.

[9] FIPS: Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, 2013.

[10] Online Trust Alliance: Cyber Incident & Breach Trends Report, Review and analysis of 2017 cyber incidents, trends and key issues to address, 01/2018.

[11] PwC: The Global State of Information Security Survey, 2016.

[12] Open Web Application Security Project (OWASP): The Ten Most Critical Web Application Security Risks, 2017.

Verimi GmbH
Oranienstraße 91
10969 Berlin | Germany
https://www.verimi.com
Phone: +49 30 20689 112
office@verimi.com