verimi

VERIMI Security

Overview of Security Features of a Cross-Industry Identity Management Platform

May 2018
White Paper

Contents

Abstract

Users today leave a digital trail in the digital world. Unlike in the analogue world, this data track remains available and retrievable for an indefinite period of time. The exposure of this user data, combined with structurally insecure technological paradigms provides ample opportunity for all kinds of misuse. This is where VERIMI kicks in. VERIMI offers secure identity management solutions based on secure technological methods, empowering the users and data owners to regain ownership of their own data and data trails. Users, companies and government bodies can be sure that interactions and transactions are being managed securely.

Following a brief introduction this white paper will examine the specific security aspects of VERIMI considering available features, technological dimensions and finally, workflow patterns as well as the organizational structure. This paper is also intended as a contribution to the professional discussion of security issues and we expressly welcome constructive feedback – please forward to security@verimi.com.

1 Introduction

Business models in the digital world are largely based on the collection, analysis and use of data that users provide or that can be acquired from users. This enables companies to closely align with user context and needs, i.e. be as specific as possible and targeting added value for users. Although personal data can be collected indirectly for these business models, these do not provide a sufficiently solid foundation for business activities that go beyond core business. It becomes increasingly necessary to draw on personal data to fulfil procedural (B2B2C, end to end) or regulatory prerequisites (anti-money laundering [AML] respectively know your customer [KYC]). But the origin and topic-related nature of this data has to be appropriately proven.

Beside their potential, the processes and technologies employed simultaneously provide opportunities for misuse – one of the drivers of the rise in security incidents witnessed in recent years[1]. Although specialised providers play a leading role in terms of developing exceptionally high security standards, many market players neither have the resources nor the expertise to meet these standards. Furthermore, challenges in terms of user-friendliness of secure processes have yet to be resolved in a satisfactory way – acceptance levels remain stubbornly low despite the good progress made in raising awareness.

The required increase in need as much as appreciation of secure solutions as well as the individually secured use of personal data in the digital space is undisputed. A holistic approach targets the systematic stabilisation by ensuring privacy (General Data Protection Regulation, GDPR, ePrivacy), strengthening trust in digital tools (e.g. eIDAS[2]), and complying with technological (security) standards (German IT Security Act [ITSiG], etc.) Alongside this, efforts should be made to balance interests driven from economic, governmental, and social perspectives.

[1] A more than fivefold increase in global incidents between 2013 and 2017, see [11] and [12].
[2] Electronic Identification, Authentication and Trust Services.

VERIMI comes into play at the intersection of the various solution elements and establishes a platform for the management of secure electronic identities as a basis for legally compliant and trustworthy Web-based business processes. The objective of VERIMI is to handle identity management on behalf of users, companies, and public authorities in a secure and user-friendly manner, fully compliant with data protection legislation. VERIMI thus bridges the gap between users on the one hand and service providers (companies and governmental bodies) on the other.

The personal data required for the various services are securely administered within the VERIMI platform. Users who wish to use the services of a specific service provider can use VERIMI to authenticate themselves securely with the provider concerned. The personal data required to provide the service is securely transmitted to the service provider by VERIMI. Two rules, in particular, are adhered to:

- Service providers only receive the identity data required for their service (purpose limitation) which are stored centrally in the VERIMI profile of the users
- Users can decide on a case-by-case basis what data is transmitted to service providers (transparency and implementation of the right to informational self-determination)

The data is solely processed for the purposes outlined above.

2 Features

The core functions of VERIMI currently primarily focus identity management, i.e. the administration of data and authorizations associated with digital identities of users with the help of software solutions. Secondly, VERIMI enables to access the online services of various providers using a single sign on process. Thirdly, users are able to administer their privacy settings on a case by case level.

The security measures implemented for these features already provide the basis for the requirements of advanced stages of security and data privacy, e.g. eID, QES or electronically available features tied to German or European identity documents (ID cards, passports, residence permits).

2.1 Identitity Management[3]

Depending on the services accessed by users via VERIMI, various identity attributes are required, e.g. last name, first name, address, and date of birth, but also telephone numbers, e-mail addresses and bank details. Users can decide at their own discretion which of their identity attributes they wish to manage via VERIMI.

[3] In Europe, eIDAS (electronic Identification, Authentication and Trust Services), which is based on the ISO/IEC 29115 international standard, sets out the regulatory framework for identity management and trust services. There is also further legislation in Germany that regulates identification processes in specific contexts, e.g. the Money Laundering Act (Geldwäschegesetz), the Telecommunications Act (Telekommunikationsgesetz), the Federal Act on Registration (Bundesmeldegesetz), and the Carsharing Act (Carsharing-Gesetz).

What matters is that the data used in VERIMI is authenticated, that it can be updated in the event of changes and that only the identity owners themselves have full make use of their data. Consequently, VERIMI's core value proposition is driven by fulfilling highest data and identity security standards, both in terms of registration and the updating of this data as well as its authentication.

2.1.1 User Registration

Users can register for VERIMI in several ways:

- Using the Video-Ident procedure offered by WebID Solutions GmbH
- Via service providers with whom the user has already securely registered

The personal data contained on the user's ID card/residence permit/ passport is recorded and then securely stored in VERIMI. Other personal data administered by users via VERIMI also has to be verified leveraging methods depending on the type of data in question. The telephone numbers of mobile devices, for instance, are verified using a confirmation text message, whereas e-mail addresses are verified using a confirmation e-mail. In the first case, a six-digit code is sent to users via the telephone number provided; this code is then verified within the VERIMI platform.

For e-mail verification, a link containing a 16-digit-alphanumeric code is sent by e-mail. Thus, all identity attributes are authentic. By linking the data with appropriate authentication methods, the identity attributes can be used securely to service providers for both identification and authentication purposes.

2.1.2 Updating Data Identity

Users' identity data can change over time, such as the user's last name if they get married, their address if they move or their bank details if they switch banks.

The update of identity attributes follows the same process as for initial user registration.

2.1.3 Locking and Unlocking Accounts

Users have two ways of locking their VERIMI account:

- Via a telephone support line: Users provide the e-mail address associated with the VERIMI account, then line staff members lock the account. The users will be informed about the blockage.
- Via the VERIMI platform: Users log in to VERIMI using one of the authentication methods at their disposal and then proceed to lock their account by themselves.

The account will also be locked if the password for the “username/password” authentication method is entered incorrectly several times. The account will initially be locked for 30 minutes following five incorrect attempts.

In all cases users will be notified via e-mail or text message that their account has been locked.

In order to unlock their VERIMI account, users sign in to VERIMI using one of their authentication options. VERIMI will send a one-time password to the cell phone number or e-mail address provided; this one-time password can be used to unlock the account.

2.2 Log-in via VERIMI

Using their VERIMI account, users can subscribe to a variety of service providers using cryptographic protocols that meet accredited security standards used in a host of different applications around the world.

Service providers only receive the identity data that they require for their service. In order to provide their services, for instance online retailers receive the identity attributes last name, first name, address, and bank details (and if required information about the user’s age).

However, users can decide at any time, what identity data they wish to share with individual service providers.

2.2.1 OpenID Connect

When subscribing to service providers via VERIMI, users use OpenID Connect as an extension of OAuth2.0 within the authorization code flow. OpenID Connect is a protocol that allows users to sign on with different service providers via the central VERIMI service platform, see also [7]. Users start by accessing the website of the service provider concerned, which directs them to VERIMI. Here, the users sign on using one of their chosen authentication methods. Please refer to Section 3.1.3 for more technical details on the tokens issued.

2.2.2 Authentication

Before they can sign in with participating service providers, users have to authenticate themselves vis-à-vis VERIMI. Two authentication methods are currently in use:

- Username/password: This process constitutes a single-factor authentication method based on the knowledge factor (password).
- VERIMI app: This process constitutes a two-factor authentication method. In this instance, a secret key is stored in a secure area of the smartphone (ownership factor), ready for use in an asymmetric challenge-response process. The secret key can only be used if the smartphone has been

unlocked (knowledge factor if entering a pin, inherence factor [biometrics] if using fingerprint or, in the future, facial recognition).

Which procedure is used depends on the security level required by the service provider. Signing up with username/password, for example, can be used to access low-security services. These low-security services might be bank transfers of smaller amounts or orders placed with online retailers. With two-factor authentication, the user could, for example, open bank accounts, transfer larger amounts and take out insurance policies.

The security experts at VERIMI work with the service providers concerned to decide which authentication method is suitable for each service.

2.3 Data Protection

VERIMI takes data protection very seriously. All systems have been developed in accordance with the “privacy by design” principle, see also [6].

2.3.1 Users

Users can decide at any time whom they wish to share each of their identity attributes with and can track which of their identity attributes they have transferred to which service providers – and when. This differentiated approach facilitates a step-wise opt-in process, as stipulated by the rules set by GDPR and ePrivacy. Beyond this, VERIMI does not analyse user activity[4], as already outlined above. All this data, including the identity attributes, is protected by means of user-specific keys (as described in Section 3.3.3).

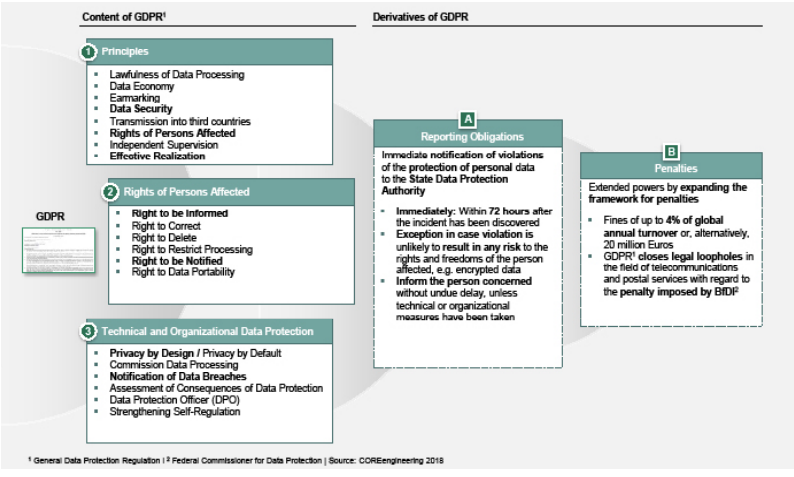

Fig. 1: Overview of General Data Protection Regulation

[4] Fraud detection can be used for analysis, anonymized analyses are performed and evaluated to improve the user experience.

2.3.2 Service Provider

Different service providers receive different user identity attributes to enable them to deliver their services. For example, a service provider providing online content for persons aged older than16/18 in line with the German Youth Protection Act (Jugendschutzgesetz) needs to know in a validated and fully reliable way whether users have reached the appropriate age, but does not necessarily require the exact date of birth or other identity data. On the other hand, online retailers shipping their goods to customers require the following identity attributes: Last name, first name, address, and potentially bank details.

Before a service provider can use VERIMI as an identity provider, the identity attributes it receives to perform its service(s) are specified. Working in conjunction with the participating service providers, the VERIMI Data Protection Officer decides which user identity attributes are absolutely necessary for the service providers to provide their service(s). No other data is transferred to this service provider.

In doing so, VERIMI follows the guidelines issued by the German Federal Commissioner for Data Protection and Freedom of Information and also takes advice from data protection officers at state level.

Whenever data is transferred, information about which service provider receives which information for their service(s) is displayed and has to be confirmed by the user. Consequently, users themselves can decide whether they wish to share this information and whether they would like to use the service (opt-in).

3 Technologies

From the beginning all VERIMI systems were designed to facilitate secure implementation of the VERIMI service (security by design). This not only encompasses the cryptographic processes used but also the technical and infrastructural, software-related and overarching elements which are used to secure the platform and are described in this section. Workflow patterns and structural/organizational elements will be described in chapter 4.

3.1 Infrastructure/Platform

All user data administered by VERIMI is protected at all times, whether within the VERIMI platform, during transmission or with the service provider. All the cryptographic processes used to protect identity data have been recommended by the German Federal Office for Information Security (BSI) and adhere to the Technical Guidelines [3] and [4] published by the BSI. Furthermore, the cryptographic processes used in VERIMI are described in a cryptographic concept devised in accordance with BSI Guidelines (see [5]).

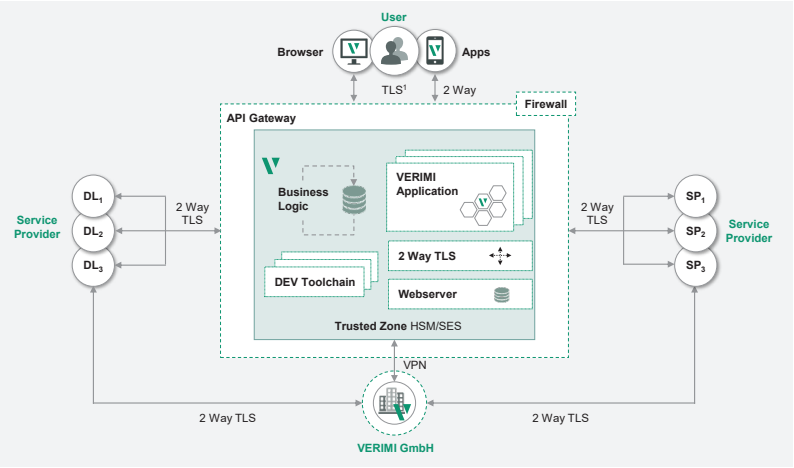

Fig. 2: Overview of VERIMI Security Architecture

If, in the future, vulnerabilities arise in the cryptographic processes and methods used, it will be possible to switch to other processes immediately. To ensure this a migration concept exists that facilitates a prompt migration to alternative processes.

3.1.1 Storage/Deletion

VERIMI administers the identity attributes transmitted by users during registration. These include last name, first name, date of birth, place of birth, telephone number(s), e-mail address(es) and bank details. VERIMI also generates and stores additional identity attributes: A UUID[5] in order to unambiguously identify users within VERIMI, several eUUIDs[6] in order to clearly identify users within service providers and, depending on the authentication method used, the user's encrypted e-mail address (if using the "username/password" method) or the public key if using two-factor authentication via the VERIMI app.

The UUID, the public key, and the encrypted e-mail address establish the "VERIMI ID," which is used within the VERIMI app.

In addition, all data transfers carried out between users and service providers via VERIMI are stored within VERIMI as long as the account exists, meaning that users can always track which of their identity attributes they have shared with which service providers, when they did so and for what purpose.

Regarding deletion users can either directly (i.e. immediately) approve the deletion of their account or for the time being just lock it. If the user does not conduct any further activity once the account has been locked, the account will be deleted automatically after six months. During the six-month grace period, the user has the option of reactivating the account and continuing to use VERIMI.

When the account is deleted, all related data and encryption keys are also deleted; what's more, the user-specific attributes are also deleted irreversibly.

[5] UUID stands for "Universally Unique Identifier.
[6] eUUID stands for "external Universally Unique Identifier." Each service provider is assigned a specific UUID in order to prevent user behavior being tracked on a cross-service basis via VERIMI.

3.1.2 Communication

All communication channels are protected by means of Transport Layer Security (TLS 1.2). These channels are:

- The communication channel between the user and the service provider
- The communication channel between the user and VERIMI
- The communication channel between VERIMI and the service provider

All data is transferred in encrypted as well as authenticated form. To this end only cipher suites recommended by BSI in [4] are used.

The respectively other party has to authenticate itself during establishment of the TLS connection. The X.509 certificates used between VERIMI and service providers were issued by trustworthy certification authorities (CAs). VERIMI only accepts certificates from the following CAs:

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

Users authenticate themselves vis-à-vis VERIMI using one of the authentication methods described in Section 2.2.2.

Communication between VERIMI GmbH and the VERIMI platform takes place via a secure VPN connection.

3.1.3 Access

OpenID Connect

Users sign on with service providers using OpenID Connect. Having successfully authenticated the user, VERIMI issues two tokens to the service provider, each of which has a singular objective:

- ID tokens contain a unique identifier that enables the service provider to identify users within its system. Each service provider receives another and different identifier in order to prevent tracking.
- Access tokens grant access to the content of the approved data groups. They are valid for 60 seconds and have to be transferred with every read or write request to the VERIMI platform.

The token is issued in exchange for the authorisation code following reciprocal authentication between the service provider and the VERIMI platform (see Section 3.1.2). This code is given to the service provider by the user once the latter has successfully signed in to the VERIMI platform. The authorisation code is a NONCE taken from the alphabet {0,..., 9,a,...,z,A,...,Z,-, _} comprised of 16 characters and with a validity period of 60 seconds. This process ensures that service providers can only access users' identity attributes once the user has approved.

ID and access tokens are JSON Web tokens (see [1]) with signed headers and payloads. The signature algorithm ECDSA-SHA384 (curve p-384, see [8]) is used to produce the signature. Alongside the content described above and a time stamp as to when they were created, the particular payloads also include a 16-character NONCE[3] taken from the alphabet {0,..., 9,a,..., z, A,..., Z, -, _}. With the signature, VERIMI confirms that the users have authenticated themselves with VERIMI and that the identity attributes transmitted are authentic.

All necessary random values (pairs of keys for the signature, random values for generating the signatures, NONCEs for the authorisation code, ID token and access token) are generated using the random number generator described in Section 3.3.3.

TWI-Factor Authentication

Two-Factor authentication (2FA) in the VERIMI apps uses the factors of knowledge and ownership or knowledge and existence. In the first case the key (ownership factor) is in the secure area of the user's smartphone, which is accessed by means of a PIN. In the second case access to the PIN is granted by means of fingerprint recognition, with facial recognition as an option in the future.

3.2 Software/Applications

3.2.1 VERIMI Web Application and Mobile Apps

The VERIMI platform consists of three core applications, each providing comprehensive functionality:

- The web application, which can be accessed via the Internet and used via any browser
- The native iOS App for optimized user experience on Apple devices
- The native Android App for optimized user experience on devices with an Android operating system

The Apps are being continuously improved. In addition to the testing for possible security vulnerabilities, the security improvements of the respective operating system are also integrated.

3.2.2 Hardening

The platform's operating system is a Linux derivative with all unnecessary functions deactivated and all security-enhancing features switched on. This includes, first and foremost, the configuration groups file system, software updates and integrity checks. The VERIMI Apps for Android and iOS are also hardened with the help of a tool: The Trusted Application Kit (TAK) created by Giesecke+Devrient features among others White Box Crypto in order to obfuscate cryptographic keys and functions, as well as 2-way TLS, secure storage, hook and root detection and device fingerprinting for accessing a smartphone.

[7] NONCE bedeutet Number Only Used Once.

3.2.3 CQRS - Command Query Responsibility Segregation

As part of the CQRS architecture the components Command (Writer) and Query (Reader) are separated from each other. This enables an independent writer and query model to be created in order to match the system‘s specific needs. For example, the fraud detection component can create an entry in the database for each invalid login attempt, while the fraud query component provides an aggregated model with a corresponding view of these invalid login attempts.

Furthermore, the CQRS structure is beneficial for applications where the typical usage pattern between writing and reading is not evenly distributed. CQRS enables more reader instances to be started in read-intensive applications, whilst only triggering one command component at the same time in order to carry the load.

3.3 Overarching Technical Elements

3.3.1 Physical Security

All IT components (servers, databases) required to implement the VERIMI service are housed in specifically secured locations. The four-eyes principle is executed by administrators as they access the premises, i.e. two persons must authenticate themselves by means of personalised chip cards and a PIN at the secured access points in order to gain access. Every time the premises are accessed, this is recorded in an audit-proof manner and regularly analysed by the VERIMI security team.

The locations are extensively secured. Furthermore, they are equipped with multi-level alarm systems, so that intrusions can be detected at any time and notification of these can be forwarded to the responsible security team.

In addition there is a two-zone model. Servers and databases used for the secure operation of VERIMI are housed in zone 1. Key management services (random number generator, storage of user-defined keys for encrypting identity attributes, keys for encrypting user name and password, and keys for signing ID and access tokens) in zone 2. Access to these IT components (server and HSM) is additionally secured by virus scanners, firewalls and intrusion detection/prevention systems and is logged and analysed separately from zone 1.

System maintenance and updates may also be carried out online by VERIMI administrators. This access to the VERIMI platform is secured via a VPN and administrators are given personalised chip cards and a PIN in order to gain access. A dual-control principle is implemented here too. Staff, who log in to the system via a VPN, require the confirmation of another person, which also logs the activities and saves them in an audit-proof manner.

3.3.2 PKI - Public Key Infrastructure

Network connections on the VERIMI platform require strong levels of authentication based on digital certificates. This comprises authentication

of the internal communication of services at VERIMI, external communication with service providers and access of administrators to the logging and monitoring system. The technical platform is based on the X.509 ITU-T standard for the Public Key Infrastructure (PKI).

The VERIMI platform uses two different PKIs: One for production and one for testing purposes. Each PKI consists of one root CA and three sub CAs for dedicated usage purposes.

The root CA on the production system is offline, i.e. the private key of the CA is deleted from the system and only available as a specially secured hard copy. The private keys of the sub CAs are stored on security chip cards, which are fraud-resistant and protected by a six-digit PIN.

3.3.3 Encryption

Data Encryption

Identity attributes and transaction data are encrypted and stored in an authenticated manner (i.e. secured against tampering) in databases along with the VERIMI ID, and individual keys are generated for all users. The AES method is used in Galois/Counter mode for encryption and authentication.

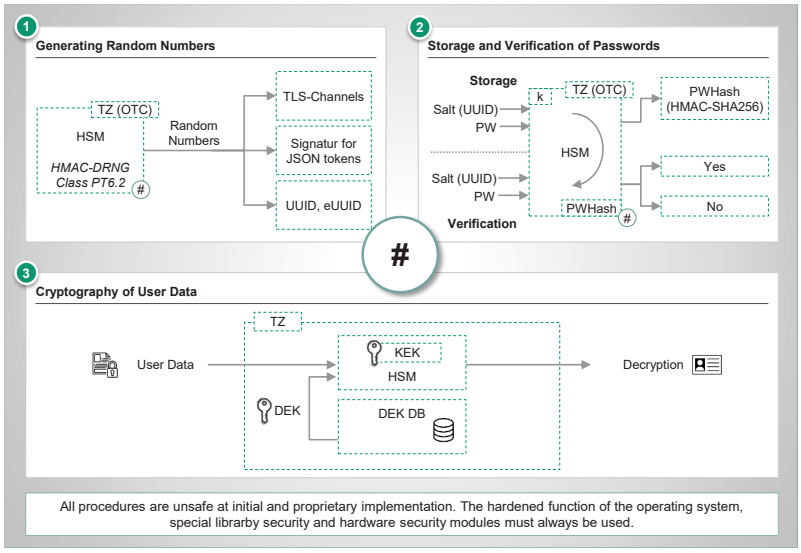

Figure 3: Overview of Methods for Generating Cryptographic Key

When users log in to VERIMI, the initial step is the determination of the UUID. When it comes to the username/password, the username (e-mail address) is searched for in the database and the UUID thus extracted. Where the two-factor authentication of the VERIMI apps is used, the public key is used to determine the UUID.

Based on the UUID, the encrypted data identity attributes required by the service provider for its service are decrypted and made available to the user; the eUUID is then provided via the ID token and the other attributes once the access token is presented.

The user passwords are not stored in clear text within VERIMI, but rather saved together with a random value (a so-called salt) and a key using HMAC-SHA256.

All keys used are 256 bits in length and are protected by a hardware security module (HSM). The HSM is located in a separately secured zone, see section 3.3.1.

Random Number Generators

The security of the cryptographic methods and protocols used depends to a large extent on the entropy (unpredictability) of the keys and cryptographic parameters used. VERIMI uses random number generators recommended by official agencies, e.g. Federal Office for Information Security (BSI) and the National Institute of Standards and Technology (NIST) for use in highly sensitive areas.

When it comes to generating the required random values, the deterministic random number generator HMAC-DRNG from [8] is used. This function is based on SHA256. DRNGs need a so-called seed to calculate random values. In order to get a high entropy of the random output values, this must also have a high entropy.

The seed is generated by means of a physical random number generator deployed into the HSM used by VERIMI and examined appropriately for this task.

3.3.4 HSM - Hardware Security Module

Communication within the VERIMI platform and with the organisation of VERIMI is completely and highly encrypted. The central encryption service is provided by means of a hardware security module (HSM), with Safenet Luna HSM 7 being used as a network HSM. The PED-based variant (Pin Entry Device) is the one normally used. The authentication of HSM roles requires external hardware tokens instead of passwords.

3.3.5 Cloud

VERIMI uses the Open Telekom Cloud (OTC), a public cloud based on OpenStack. OTC is an infrastructure-as-a-service (IaaS)-solution that provides access to virtual IT infrastructures via the Internet. VERIMI can carry out the following functions autonomously within the OTC Virtual Data Center:

- Calculate resources (self-managed VMs)
- Network resources (virtual data centers (VPCs, DHCP, DNS, firewalls))
- Dynamic load handling (elastic load balancing and automatic scaling)
- Storage resources (block and object storage)
- Backup and data redundancy strategies
- Database services (relational database service)
- Container services (cloud container engine)
- Monitoring and notifying (cloud eye)
- Network protection (e.g. anti-DDoS)

3.3.6 Intrusion Detection and Prevention

VERIMI uses various virus scanners and firewalls to protect itself from external attacks. Virus signatures and firewall configurations are regularly updated and adapted according to the current security situation.

Nevertheless, these measures alone are not enough to protect the platform. For instance so-called zero day exploits (vulnerabilities that were previously unknown) are not recognized. In order to be able to respond to new attacks, various intrusion detection and prevention systems have been implemented within the VERIMI platform. These can detect attacks by means of identifying anomalies and then initiate appropriate countermeasures.

Furthermore, all activities are recorded, stored and regularly inspected by security experts regarding incidents using established tools regarding anomalies, thereby ensuring an additional manual check of the system‘s security.

3.3.7 ISMS - Information Security Management System

VERIMI aims to be certified in accordance with ISO 27001 by the end of 2018. A data protection management system (DMS) and a compliance management system (CMS) will be implemented in addition to the ISMS.

4 Organisation

Besides using technical measures to secure data, organisational and personnel measures aimed at ensuring the secure operation of VERIMI must be implemented too.

The security measures required are not only developed and implemented by internal subject matter experts assisted by renowned research institutions, but are also assessed externally in order to determine their completeness and effectiveness, see Appendix A.

Security measures are developed based on tried-and-tested procedural models. This includes implementing the latest security measures as well as activities to ensure business continuity (e.g. crisis management, procedures for security incidents and measures to update in accordance with the current security situation).

4.1 Structure

4.1.1 Security Team

The security team consists of an information security officer and several security experts.

Besides developing organisational, technical, infrastructural and staff security measures, they also implement these measures as well as ensure uninterrupted operations. Not only do all VERIMI employees attend regular trainings, they also have to adapt to the current security situation in order to be able to react to any possible security incidents.

VERIMI‘s security is continuously being improved, with renowned research institutions supporting best practice implementations: The Fraunhofer Institute AISEC and the Identity Management Working Group of the Free University of Berlin.

4.1.2 Reliability Testing

All VERIMI employees are thoroughly examined prior to recruitment with regard to their qualifications for the tasks for which they will be responsible. Training and previous employment are checked based on training certificates and employer testimonials. Furthermore, all prospective employees must submit a clearance certificate issued by the police.

4.1.3 Security Training

VERIMI regularly conducts security training to raise awareness of IT security and data protection. Training is not only mandatory for VERIMI’s technical staff (for example, system administrators and developers) but for the administrative staff as well. And it is adapted for the specific requirements of the respective staff group. It covers all relevant aspects of IT security and data protection, from current threats to specific attack patterns (including social engineering) and the consequences of successful attacks, as well as risk mitigation methods.

Furthermore, as part of the annual Campus Week, renowned researchers are invited to present their current research topics and discuss their results. Gaining an insight into innovative technologies enables VERIMI to continually improve its security.

4.1.4 Security Related Roles

Data Protection Officer

In accordance with the European Commission‘s new General Data Protection Regulation, VERIMI has appointed a data protection officer. The data protection officer is not only supported by a team of qualified employees, but also by renowned scientific institutions. With regard to data security, the data protection team works closely with the VERIMI security team.

Information Security Officer

VERIMI has appointed an Information Security Officer (ISO), whose main responsibilities include:

- Aligning information security targets with board of management
- Coordinating and planning information security together with the Information Security Team (IST)
- Developing and maintaining guidelines and regulations regarding information security in the company
- Advising the board of management on information security issues
- Documenting information security measures
- Training employees in information security
- Planning and developing incident management and preemptive crisis management (including an emergency plan and handbook)

Compliance Officer

VERIMI has appointed a Compliance Officer (CO). The CO has the task of implementing VERIMI compliance regulations in the corporate structure and business processes by setting up a compliance management system. With the knowledge of the company structure as well as the operational processes and products, they identify company-specific risks in terms of legal breaches are identified as part of a systematic risk analysis process.

4.2 Processes

4.2.1 Software Quality in the Development Phase

When developing software used for implementing the VERIMI service, focus is placed on the quality of the software in order to minimize security vulnerabilities resulting from software errors. The software must undergo several quality assurance tests before being used in the existing system.

One focus is on preventing known attacks such as the OWASP top compilations.

4.2.2 Penetration Testing

As exhaustive tests and clear specifications cannot completely rule out errors, penetration tests are carried out regularly in order to be able to identify and correct security gaps at an early stage.

An established model is used to control penetration tests, which are based on analysing the degree of risk (based on probability and extent of the technical and business-related impact). Both internal and external resources are used to carry out penetration tests.

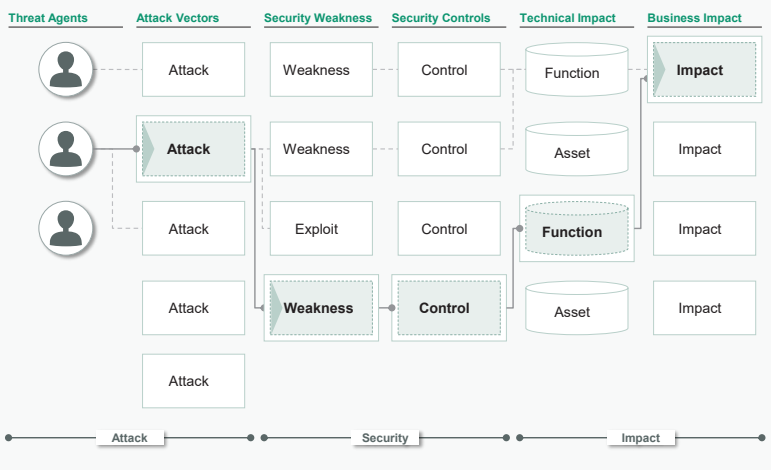

Fig. 4: Risk assessment model for attack vectors, see [10]

4.2.3 Vulnerabilities Management

Software can contain errors. Some of these errors may also lead to security vulnerabilities. The same applies for all security measures implemented, be they staff-related, organizational, technical or infrastructural. Despite evaluating these security measures, there may be security vulnerabilities may prevail that were not identified as a result of this process.

The security team therefore regularly reviews the effectiveness of the measures implemented, which involves simulating their own attacks (hacking, but also phishing attacks etc.), thereby testing the effectiveness of security measures and training.

4.2.4 Procedure for Handling Security Incidents

Should there be security vulnerabilities, e.g. ones identified by the team or those arising from actual attacks, the security team will have dry-run possible attack scenarios and prepared appropriate countermeasures. These can range from short-term shutdown of safety-critical services to shutting down the entire platform until safety is restored.

Furthermore, the current security situation is regularly monitored. Other sources, e.g. the Computer Emergency Response Team of the German Federal Office for Information Security, provide information on current security breaches and attacks in order to enable initiation of appropriate countermeasures.

4.2.5 Evaluation and Certification

All VERIMI infrastructure components are evaluated and certified according to renown models of procedure. This process checks whether security

measures have been implemented appropriately for all security risks, as well as how effective these measures are (i.e. whether they adequately mitigate risks). The scope does not only include the current state of implementation, but also whether VERIMI is enabled to react appropriately to security incidents and current developments upon attack.

VERIMI Apps

VERIMI Apps are software for smartphones that users can use to securely authenticate themselves by means of a username/password or with a two-factor authentication using VERIMI (and thus via OpenID Connect in the case of service providers, see section 2.2.1). VERIMI aims at certification of these Apps in accordance with common criteria EAL 4.

EAL is the abbreviation for Evaluation Assurance Level. The criteria of EAL 4 demands that the App is methodologically developed, tested and reviewed, thus being highly likely to fulfill the security functionality of which it claims to be capable.

VERIMI GmbH and Platform

By carrying out extended risk analysis, VERIMI is aiming for a BSI baseline protection certification. This also includes certification in accordance with ISO 27001. The plan is to achieve certification by late 2018, which will then be renewed for each subsequent release.

Certification covers both the IT infrastructure operated by VERIMI GmbH and the platform operated by VERIMI.

4.2.6 BCM - Business Continuity Management

By carrying out extended risk analysis, VERIMI is aiming for a BSI baseline protection certification. This also includes certification in accordance with ISO 27001. The plan is to achieve certification by late 2018, which will then be renewed for each subsequent release.

Certification covers both the IT infrastructure operated by VERIMI GmbH and the platform operated by VERIMI.

Business Continuity Management (BCM) protects VERIMI from serious damage or existential threats in the case of an emergency. This also applies to external service providers via VERIMI. It describes specifications in terms of content, staff and organisation and procedures for crisis management aimed at:

- Ensuring the continuation of time-critical activities and processes in the event of an emergency
- Avoiding damage wherever possible by implementing appropriate measures
- Reducing the impact of damage incurred
- Supporting a quick and orderly recovery of normal operation

The Crisis Management Officer for VERIMI is appointed, and the terms as well as the processes based on the principle of “plan-do-check-act” defined. The emergency manual describes the strategies in the event of a crisis while taking into account defined emergency scenarios and their criticality. Specifications and details are described in the Business Continuity Management guideline.

5 Conclusion

Security in the digital world is currently one of the most urgent topics. VERIMI addresses this topic in three ways:

- As a service, VERIMI provides a secure identity management platform that allows users to securely manage their digital identity and provides service partners with secure digital identities
- With regard to the internal construction of production, VERIMI relies on safe technologies and current best practices in-line with continuous development and improvements
- Finally, in terms of the social dimension, VERIMI can act as an emancipation tool, handing back to users sovereignty and control over their personal data

It is of paramount importance to discuss these dimensions. Since the dimensions are characterized by a significant dynamic force, both individually and overall, it is not only permanent adaptations to the technological level that are important, but also aspects of functionality and social development. The debate must be conducted from an economic, political, civil and technological point of view – while reconciling the interests of these groups.

Appendix

A. Support

VERIMI is continuously being developed and tested in terms of its security. Two research institutions are providing support in this regard: The Identity Management Working Group at the Freie Universität Berlin, headed by Prof. Marian Margraf, and the Fraunhofer Institute for Applied and Integrated Safety (AISEC), headed by Prof. Claudia Eckert. Furthermore, COREengineering is acting as a development partner for the development and operationalisation of the security functions.

Freie Universität Berlin

The ID Management Working Group at the Freie Universität Berlin deals with the design, creation and evaluation of usable and secure software and IT systems.

The main research topics of the working group include:

- Physical unclonable functions
- Asymmetric and symmetric crypto-analysis
- Usable security
- Intrusion detection systems
- IT security management, security management as a service

Fraunhofer AISEC

Fraunhofer AISEC supports companies in all industries and service sectors in securing their systems, infrastructures, products and services. On behalf of customers, it develops high-quality security technologies in order to increase the reliability and trustworthiness of IT-based systems and products and is geared towards reducing manipulation. Approximately 80 scientific and technical employees of Fraunhofer AISEC develop optimally tailored concepts and solutions ranging from economic needs, user-friendliness and safety requirements. The security-testing laboratories are equipped with state-of-the-art equipment, and highly qualified security experts evaluate and analyse the safety of products, hardware components as well as software products and applications. Functionality, interoperability, conformity and compliance tests are carried out in the laboratories and customers are provided with targeted advice. Customers include manufacturers, suppliers from industries including chip card systems, telecommunications, the automotive industry and its suppliers, logistics and aviation, mechanical engineering and automation technology, healthcare, the software industry, the public sector and eGovernment.

COREengineering

As part of CORE SE, COREengineering supports companies in industries featuring an above-average contribution of information technology to the value chain. COREengineering acts at the interface between technical requirements and system development. The experts at COREengineering ensure the high-quality planning and control of agile development projects based on innovative IT architectures.

Analysing challenges and developing solution patterns are as much a part of the scope of services as the design of IT architectures, the orchestration of coding and integration as well as the transfer of production to open cloud systems. As a result, COREengineering implements high-performance software systems for mission-critical business areas, providing clients with significant efficiencies in IT management while maintaining market-specific competitive advantages.

B. References

[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 Schlüssellängen, 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

COREengineering
Am Sandwerder 21-23
14109 Berlin | Germany
https://engineering.core.se
Phone: +49 30 26344 020
office@core.se