## Security requirement

# Enterprise Service Bus

Deutsche Telekom Group

| | |
|---|---|
| Version | 2.2 |
| Date | Jul 1, 2020 |
| Status | Released |

# Publication Details

Published by
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Germany

| | | |
|---|---|---|
| File name | Document number<br>3.13 | Document type<br>Security requirement |
| Version<br>2.2 | State<br>Jul 1, 2020 | Status<br>Released |
| Contact<br>Telekom Security<br>psa.telekom.de | Validity<br>Jul 1, 2020 - Jun 30, 2025 | Released by<br>Stefan Pütz, Leiter SEC-NIS |

Summary
Enterprise Service Bus

# Table of Contents

# 1. Introduction

This security document has been prepared based on the general security policies of the Group.

The security requirement is used as a basis for an approval in the PSA process, among other things. It also serves as an implementation standard for units which do not participate in the PSA process. These requirements shall be taken into account from the very beginning, including during the planning and decision-making processes. When implementing these security requirements, the precedence of national, international and supranational law shall be observed.

If compliance with the described requirements can not be achieved or is only partially feasible in individual cases, a risk assessment must be carried out together with a Security- and/or Data Privacy Expert (in accordance with the relevant requirement) and possible alternative protective measures agreed.

# 2. Authentication

Req 1 Enterprise Service Bus and all service consumers and service providers must be mutually authenticated. The connecting partner application is responsible for the correct and secure implementation of his services.

No plain-text protocols must be used during authentication. A suitable process may be, for instance, implementation with the help of certificates and a PKI. If communication takes place beyond network boundaries, cryptographically strong mechanisms must be used.

*Motivation: Only proper authentication can ensure that the information provided is read solely by the designated consumer or is generated by the authentic provider.*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Disruption of availability

ID: 3.13-1/2.2

Req 2 The service repository must clearly identify all access to the repository.

*Motivation: A service repository (or also registry) includes information on which service consumer may communicate with which service provider. Weak authentication could make it easier for misuse scenarios to occur in the service repository.*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data

ID: 3.13-2/2.2

Req 3 End users must not be authenticated directly at the ESB but only via proxy mechanisms or portals.

Service providers and service consumers are solely machines.

*Motivation: If end users could access the ESB's infrastructure, comprehensive measures must be implemented to ensure that only these end users have access to the secure ESB infrastructure. The consequence is extremely time-consuming firewall administration for thousands of call-center agents, as well as possible administration of thousands of client certificates for authentication.*
*The absence of any direct physical access to the ESB on the part of end users substantially reduces the risk of end users potentially exploiting bus vulnerabilities.*

For this requirement the following threats are relevant:
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.13-3/2.2

Req 4 User accounts must be used that allow unambiguous identification of the user.

Users must be identified unambiguously by the system. This can typically be reached by using a unique user account per user. So named group accounts, i.e. the use of one user account for several persons, must not be used. One exception of this requirement are so named machine accounts. These will be used for authentication and authorization from system to each other or for applications on a system and can’t be assigned to a single person. Such user accounts must be assigned on a per system or per application basis. In this connection, it has to be guaranteed that this user account can’t be misused. Possibilities to protect these accounts against misuse are:

- Configuring of a Password that fulfils the security requirements and is known by less than possible circle of administrators.

- Configuring the user account that only a local use is possible and a interactive login isn’t possible.
- Use of a technique for authentication of the specific user account with public and private key or certificates.
- Limiting the access over the network for legitimized systems.

Additional solution must be checked on their usability per individual case.

*Motivation: Unambiguous user identification is mandatory to assign a user rights that are necessary to perform the required tasks on the system. This is the only way to adequately control access to system data and services and to prevent misuse. Furthermore, it makes it possible to log activities and actions on a system and to assign them to individual users.*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized use of services or resources
- Denial of executed activities

ID: 3.01-13/3.0

| Req 5 | User accounts must be protected against unauthorized use by at least one authentication attribute. |
|---|---|

The various user and machine accounts on a system must be protected from misuse. To this end, an authentication attribute is typically used, which, when combined with the user name, enables unambiguous authentication and identification of the authorized user.
Authentication attributes include:

- Cryptographic keys
- Token
- Passwords
- PINs

This means that authentication based on a parameter that can be spoofed (e.g. phone numbers, public IP addresses or VPN membership) is not permitted. Exceptions are attributes that cannot be faked or spoofed by an attacker. Two of the above options can be combined (2-factor authentication) to achieve a higher level of security. Whether or not this is suitable and necessary depends on the protection needs of the individual system and its data and must be evaluated for individual cases.

In companies of Deutsche Telekom group where the MyCard or a comparable smartcard is available this solution should be preferred.

*Motivation: User accounts that are not protected with a secret authentication attribute can be used by an attacker to gain unauthorized access to a system and the data and applications stored on it.*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized use of services or resources
- Denial of executed activities

ID: 3.01-14/3.0

| Req 6 | User accounts with extensive rights must be protected with two authentication attributes. |
|---|---|

User accounts, for example used for administration, maintenance and troubleshooting, have extensive rights. Extensive rights means that with an appropriate user account changes like writing, reading etc. to system parameter and configurations are possible. Therefore a single protection (e.g. a password), as for normal user accounts with less rights, is not suitable. To get a higher protection level it is necessary to use two independent authentication attributes. For this a combination of an attribute that the user knows and an attribute that the user owns will be used often. This kind of authentication will be named as 2-factor authentication. Examples for 2-factor authentication are:

- Smartcard (e.g. MyCard) with PIN
- Private key with passphrase

- Token for one-time passwords

In companies of Deutsche Telekom group where the MyCard or a comparable smartcard is available this solution should be preferred.

*Motivation: User accounts with extensive rights as used for system administration have a higher risk for system's security. An attacker can get extensive rights by compromising such an user account to get access to wide parts of the system and stored data.*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized use of services or resources
- Denial of executed activities

ID: 3.01-15/3.0

| | |
|---|---|
| Req 7 | Predefined and not used user accounts must be deleted or disabled. |

Many systems have default and not used user accounts (e.g. guest, ctxsys), some of which are preconfigured with or without known passwords. These standard users must be deleted or disabled. Should this measure not be possible the user accounts must be locked for remote login. In any case disabled or locked user accounts must configured with a complex password (12 character and more, use of upper/lower case, numbers and special characters). This is necessary to prevent unauthorized use of such a user account in case of incorrect configuration.

Exceptions to this requirement to delete or disable user accounts are accounts that are used only internal on the system involved and that are required for one or more applications on the system to function. Also for this user accounts remote access or local login must be forbidden to prevent a abusive use by users of the system.

*Motivation: Standard users are typically generally known and can be used by an attacker for targeted brute force and dictionary attacks. Standard user accounts represent a special risk if they do not use a password or only use a standard password that is generally known. Such standard user accounts can easily be exploited by an attacker in order to gain access to the system involved without being authorized to do so.*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized use of services or resources
- Denial of executed activities

ID: 3.01-16/3.0

| | |
|---|---|
| Req 8 | Predefined authentication attributes must be deleted or disabled. |

Normally, authentication attributes such as password or cryptographic keys will be preconfigured from producer, vendor or developer of a system. Such authentication attributes must be changed to an attribute not known by other parties.

*Motivation: Authentication attributes like password or cryptographic keys preconfigured from third parties are not trustable. Such authentication attributes can be used to compromise systems or their data.*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized use of services or resources
- Denial of executed activities

ID: 3.01-17/3.0

| | |
|---|---|
| Req 9 | The system must be connected to a central system for user administration. |

Systems must be connected to a central system for user administration. A solution for identity management should be preferred.
Accounts and their rights will be administrated on central identity management systems (e.g. cIAM, WiW, ZAM) in

Deutsche Telekom Group. The system must provide a central interface (e.g. LDAPs for authorization, Kerberos for authentication, locking information for certificates) or decentralized mechanisms (e.g. public-key authentication) for the provisioning ot authorization data. In areas where a central identity management system is not available a central system such as LDAP, TACACS+ or Radius server for the administration of accounts and their authentication and authorization must be used.

Exceptions to this requirement are accounts that are used only internal on the system involved and that are required for one or more applications on the system to function. Also for this accounts remote access or local login must be forbidden to prevent a abusive use by users of the system.

*Motivation: Central administration of identity of accounts and their rights means that they only have to be maintained once instead of separately on each system. From the aspect of security, the advantage is that an user account and its rights only known on a single central side. This information can be transmitted from a central side to systems (provisioning), central administrated (reconciliation) and central deleted (deprovisioning). This reduces the risk of accounts being forgotten during changing or deletion since they are configured on multiple systems. This could give a user wrong system rights or continued access to a system.*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

ID: 3.01-19/3.0

# 3. Authorization

| Req 10 | The Enterprise Service Bus must authorize the access by service consumers to service providers, e.g., with the aid of information from the repository. |
|---|---|

Service consumers that communicate with the ESB must be verified in terms of their authorization. This information is usually stored in a service repository.

*Motivation: Access monitoring can ensure that only authorized entities access the bus or the involved systems, thus preventing data theft.*

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

ID: 3.13-4/2.2

| Req 11 | Access monitoring of the ESB must follow the 'default deny' principle, i.e. access to a service must not be granted without explicit permission. |
|---|---|

*Motivation: Unnecessary access rights increase the risk of compromising the system and should therefore be avoided.*

For this requirement the following threats are relevant:
- Unauthorized use of services or resources

ID: 3.13-5/2.2

# 4. Confidentiality and data protection

| | |
|---|---|
| Req 12 | In the case of services with data protection class 3 information (e.g. credit-card data, passwords, etc.), the relevant payload data must be encrypted end-to-end in order to ensure continuous encryption for these confidential data fields. |

*Motivation: If these data are not encrypted end-to-end but merely on the transport layer, this information is then available in plain text as soon as the TLS connection is terminated or if the data are not transported (e.g., in an unencrypted message queue).*

Implementation example: Web Service Security enables individual attributes of a message to be encrypted end-to-end. XML encryption and XML signature can be applied to individual attributes in order to ensure the confidentiality of the particular piece of data, while at the same time having the option of, for instance, transforming the rest of the message.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

ID: 3.13-6/2.2

| | |
|---|---|
| Req 13 | The ESB must ensure the integrity of all messages. This means that the integrity of the entire communication between service providers, service consumers and ESB must be protected, e.g., with the aid of XML signatures. |

*Motivation: An inadequate integrity check can expose systems to certain risks such as tampering or repudiation. Changed messages can also compromise or destroy systems. For instance through XML bombs, XPath injection, SQL injection, XSS, etc.*

For this requirement the following threats are relevant:
- Unauthorized modification of data
- Denial of executed activities

ID: 3.13-7/2.2

| | |
|---|---|
| Req 14 | Data with need of protection must be protected against unauthorized viewing and manipulation during transmission and storage. |

Adequate security measures for transmission and storage of sensitive data must be implemented. The chosen measure depends on the classification for the data (e.g. following data privacy rules) and other factors such as the type of network used during transmission, the storage location for data, etc. Additionally it must be guaranteed that confidential data is not unprotected during temporary storage (e.g. web cache, temporary folders).

All authentication data such as passwords, PINs, etc. must be protected against unauthorized viewing and manipulation. This applies equally to storage and transmission.

Files of a system that are needed for the functionality must also be protected against manipulation. This is necessary because system’s integrity can be damaged when unauthorized change of these files possible is. An example is the use of cryptographic methods to validate if e.g. firmware images, patches, drivers or kernel modules are free of manipulations.

For transmission of data with a need of protection network protocols that are insecure due to insufficient security measures shall not be used. Examples are: SSLv3, SSHv1, FTP, Telnet, SNMPv1 and 2c. In case of these protocols a newer version without vulnerabilities or a secure alternative must be used.

*Motivation: If data with a need of protection is not secured an attacker could record or manipulate the data during transmission over a network. An example is the recording of user names and passwords during system administration with the telnet clear-text protocol. Storing data on a system without adequate protection may mean that unauthorized users can copy or modify it. One example is passwords stored without proper encryption on a system.*

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

ID: 3.01-7/3.0

---

| | |
|---|---|
| Req 15 | Sensitive information must not be contained in files, outputs or messages that are by unauthorized users accessible. |

Information with need of protection must not be accessible in files, outputs or messages of the system by unauthorized users. This includes information relating to the operating system, used middleware or applications such as vendor, product name, product identifier, installed software versions, installed service packs, patches, hot fixes and serial numbers. Examples for system messages which must be free of sensitive data are:

- Comments in downloadable files
- Error and system messages
- Stack traces
- Network protocols
- Login windows and dialogs

Details of implementation and information relating, e.g., to backend software/systems, function calls, SQL instructions or structure of database, must not be contained in error messages. Excluded from this are displays and outputs that can be viewed and retrieved by authorized users who are logged in. In addition, an internal transfer of system internal information for error analysis is allowed in an adequate dimension. In this case the continuative regulations or guidelines (e.g. of data privacy) must be noticed.

*Motivation: The information named above can be used by an attacker to prepare specific attacks on a system. In this way an attacker could, for example, use the precise software version to identify vulnerabilities in the product and, in a second step, exploit them.*

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.01-8/3.0

# 5. Availability

| | |
|---|---|
| Req 16 | The ESB must monitor service usage and must reject invalid queries at the first possible opportunity and raise an alarm. |

The ESB servers, routers, firewalls and other involved components should be monitored and trigger alarms in case clear threshold values are exceeded.

*Motivation: The early rejection of invalid requests conserves resources and ensures that any harmful code is not transported further into internal systems.*

For this requirement the following threats are relevant:
- Disruption of availability

ID: 3.13-8/2.2

| | |
|---|---|
| Req 17 | The system must be robust against overload situations. |

A system must provide security measures to deal with overload situations. In particular, partial or complete impairment of system availability must be avoided. Potential protective measures include:

- Restricting of available RAM per application
- Restricting of maximum sessions for a Web application
- Defining the maximum size of a dataset
- Restricting CPU resources per process
- Prioritizing processes
- Limiting of amount or size of transactions of an user or from an IP address in a specific time range

Note: A system cannot defend itself against attacks with high data volume also named distributed denial of service attacks. To defend this kind of attacks an external network based solution is necessary.

*Motivation: Attackers try to force a overload situation on a system with denial of service attacks. If such an attack is successful the availability can be compromised and integrity of system can be influenced.*

For this requirement the following threats are relevant:
- Disruption of availability

ID: 3.01-9/3.0

| | |
|---|---|
| Req 18 | If an overload situation cannot be prevented, the system must act in a predictable way. |

A system must be built in this way that it can react on a overload situation in a controlled way. However it is possible that a situation happens where the security measures are not longer sufficient.

In such case it must be ensured that the system cannot reach an undefined and thus potentially insecure state. In an extreme case this means that a controlled system shutdown is preferable to uncontrolled failure of the security functions and thus loss of system protection.

*Motivation: With denial of service attacks an attacker can try to overload a system to effect its availability or integrity. Unpredictable acting of the system can be a threat for its own functionality and data and possibly also for other systems.*

For this requirement the following threats are relevant:
- Disruption of availability

ID: 3.01-10/3.0

| | |
|---|---|
| Req 19 | The system must be robust against unexpected input. |

During data input it is necessary to validate this before processing. This includes all data which are sent to the system. Examples for this are user input, values in arrays and content in protocols. The following typical implementation mistakes must not be done:

- No validation on the lengths of transferred data
- Incorrect assumptions about data formats
- No validation that received data complies with the specification
- Insufficient handling of protocol errors in received data
- Insufficient restriction on recursion when parsing complex data formats
- White listing or escaping for inputs outside the values margin

*Motivation: An attacker can try to put a system in an unsecure state through targeted manipulation of transmitted data. The object of such an attack is to compromise the usability, availability or integrity of individual services or of the entire system. For instance a unclean memory handling can lead to a buffer overflow that allows an attacker to execute arbitrary code on the effected system.*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized use of services or resources
- Disruption of availability

ID: 3.01-11/3.0

---

Req 20 Security relevant events must be logged with a precise timestamp and a unique system reference.

Systems must log the occurrence of security-relevant incidents. So that these events can be evaluated and classified, they must be logged together with a unique system reference (e.g., host name, IP or MAC address) and the exact time the incident occurred ("Timestamp"). Exceptions of this requirement are systems for which logging cannot be implemented because of building techniques, use case or operation area. Examples for these kind of systems are customer devices such as Smartphone’s or IADs/home gateways (e.g. Speedport).

The Timestamp of a logged event must contain at least the following information:

- date of the event (Year, Month, Day)
- time of the event (Hours, Minutes, Seconds)
- Timezone, those information belongs to

Logging must be done considering the currently valid legal, wage and company regulations. Following these regulations logging of events is only allowed for a defined use case. Logging of events for doing a work control of employees is not allowed.

Typical event that reasonable should be logged in many cases are:

| **Event** | **Event data to be logged** |
|---|---|
| Incorrect login attempts | • User account,<br>• Number of failed attempts,<br>• Source (IP address) of remote access |
| System access with accounts with administrator rights | • User account,<br>• Access timestamp,<br>• Length of session,<br>• Source (IP address) of remote access |
| Account administration | • Administrator account,<br>• Administered user account,<br>• Activity performed (configure, delete, enable and disable) |

| | |
|---|---|
| Change of group membership for accounts | • Administrator account,<br>• Administered user account,<br>• Activity performed (group added or removed) |
| Critical rise in system values such as disk space, CPU load over a longer period | • Value exceeded,<br>• Value reached<br>(Here suitable threshold values must be defined depending on the individual system.) |

Logging of additional security-relevant events may be meaningful. This must be verified in individual cases and implemented accordingly where required.

*Motivation: Logging security-relevant events is a basic requirement for detecting ongoing attacks as well as attacks that have already occurred. This is the only way in which suitable measures can be taken to maintain or restore system security. Logging data could be used as evidence to take legal steps against attackers.*

For this requirement the following threats are relevant:
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 3.01-29/3.0

| Req 21 | Security relevant logging data must be send to an external system direct after their creation. |
|---|---|

Logging data must be forwarded to an external system in appropriate logging files as well as being stored locally. Standard protocols like Syslog, SNMPv3 must be preferred.

*Motivation: If logging data is only stored locally it can be manipulated by an attacker who succeeds in compromising the system in order to conceal his attack and any manipulation he has performed on the system. This is the reason why the forwarding must be done immediately after the event occurred.*

For this requirement the following threats are relevant:
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 3.01-30/3.0

# 6. ESB architecture

| | |
|---|---|
| Req 22 | ESB components must be placed in a separate network segment. This segment (e.g. VLAN) must not be accessible directly from the Internet or intranet. |

Steps must be taken to ensure that only components of the ESB are part of this VLAN.

*Motivation: Virtually all of Deutsche Telekom's EAI communication runs via the various ESBs, with extremely sensitive data passing over this infrastructure. Therefore only those components need to be combined in a network segment that belong directly to the ESB, in order to minimize the number of wanted and potentially unwanted accesses to these sensitive systems.*

Implementation example: A VLAN can ensure that only ESB components are located within a network segment.

For this requirement the following threats are relevant:
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.13-9/2.2

| | |
|---|---|
| Req 23 | The individual components of the ESB must be protected by firewalls/packet filters that are governed by a default deny policy. |

*Motivation: The ESB architecture contains critical systems and security can be supported through restrictive firewall rules.*

For this requirement the following threats are relevant:
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.13-10/2.2

# 7. ESB management

| | |
|---|---|
| Req 24 | The enrolment of new consumers or providers must be approved by centralized security/change management. |

The contract for using the services is mapped in this process, where also the Security department must be involved.

*Motivation: A stringent change process can ensure that no unauthorized parties connect to the bus.*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized use of services or resources

ID: 3.13-11/2.2

| | |
|---|---|
| Req 25 | Administrative access to the ESB's components must be provided via jump hosts or the Admin LAN. |

*Motivation: Access to the ESB's components from the Office LAN ist not allowed, because direct end user's access from outside the ESB infrastructure would be given. A connection through a jump host terminates the direct physical access to this host and also facilitates logging of administrative and other critical activities.*

*Alternatively the access can be maintained through the Admin LAN. All needed ports (e.g. SSH Port 22) is filtered/ blocked towards the Office LAN and open towards the Admin LAN.*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.13-12/2.2

# 8. System hardening

| Req 26 | Unused services and protocols must be deactivated. |
|---|---|

After installation of systems and software products local or remote reachable services and protocols are may be active, which are not necessarily needed for operation and functionality of the system. These include also services and protocols which may not be used in Deutsche Telekom Group networks on account of known security vulnerabilities. Such services and protocols must be completely disabled on the system. Additionally it is important that protocols and service are still deactivated after system reboot.

This kind of system hardening must be done before the system is reachable from the network. Otherwise an attacker has the possibility to attack and maybe compromise the unsecured system.

*Motivation: Services and protocols that are not required for system operation increase the potential attack surface and thus the risk of the system being compromised. This risk is further increased by the fact that a security inspection and an appropriate optimization of the configuration for unused services and protocols will not be done.*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized use of services or resources
- Disruption of availability
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.01-1/3.0

| Req 27 | The reachability of services must be restricted. |
|---|---|

Typically services that are enabled in the basic configuration are enabled on all interfaces of the system and can be reached from networks where the connectivity is not necessary. This availability is often not needed or meaningful for the function of a system. For this reason, services should only be enabled on interfaces where their usage is required. On interfaces were services are active,  the reachability must be limited to legitimate communication peers. This limitation must be realized on the system itself without measures (e.g. firewall) at network side.

*Motivation: Disabling services on interfaces which do not require system accessibility or by limiting the reachability can reduce the potential attack possibilities offered to an attacker. For example, access to a system via SSH from the Internet is not necessary. Is this service still accessible from Internet, this would increase the risk of attacks on the service.*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized use of services or resources
- Disruption of availability
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.01-2/3.0

| Req 28 | Unused software must not be installed or must be uninstalled. |
|---|---|

During installation of a system often software components will be installed or parts of software will be activated which are not needed for the operation or functionality of the system. This includes also parts of a software, which will be installed as examples but typically not be used (e.g. default web pages, example databases, test data). Such components should not be installed or must be eliminated after installation. Additionally is it not allowed to install software on a system that is not needed for operation, maintenance or function of the system.

*Motivation: Vulnerabilities in software of a system offer an attack window for attackers to infiltrate the system. Uninstalling components that are not required can therefore reduce the amount of possible attacks.*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Disruption of availability

ID: 3.01-3/3.0

| | |
|---|---|
| Req 29 | Unused functions of the operated software and hardware must be deactivated. |

During installation of software and hardware often functions will be activated that are not necessarily needed for operation or function of the system. Functions of software are currently inherent part which could not be deleted or deinstalled individually. Such functions must be deactivated in the configuration of the system permanently.

Beside the functions of the software also hardware functions are active which are not necessary for a system. Functions like unused interfaces must permanently deactivated. Permanent means that they must not be reactivated again after system reboot.

*Motivation: The hardware or software of a system often contains functions which are not used and so will be a risk for system security. Such functions give an attacker the possibility to manipulate the system. It is also possible to get unauthorized access to other areas or data of the system. An example is a debugging function in software which can be used for troubleshooting but must not be activated during normal operation. Or a unused hardware interface that is not secured an allows possibly unauthorized access to the system.*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Disruption of availability

ID: 3.01-4/3.0

# 9. System update

| Req 30 | Software and hardware components that are no longer supported by vendor, producer or developer must not be used. |
|---|---|

Only those operating system, middleware and application software and hardware components may be used on a system which are supported by the vendor, the producer, the developer (this includes open source communities) or other contractual partner of Deutsche Telekom AG. Components that have reached end-of-life or end-of-support must not be used. Excluded are components that have a special support contract. This contract must guarantee the correction of vulnerabilities over components lifetime.

*Motivation: Hardware and software components that have reached end of life or end of support represent a risk for a system. This means that a vendor does not supply remedial updates or patches for a component should errors or vulnerabilities occur. This means that vulnerabilities cannot be fixed when they occur and could be exploited to compromise the system or to impair its availability.*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Disruption of availability

ID: 3.01-5/3.0

| Req 31 | Emerged vulnerabilities in software and hardware of a system must be fixed or protected against misuse. |
|---|---|

Prior to installation of a software or hardware component, users must check whether any vulnerability has been discovered and published for the version they are installing. Any component that proves to have a vulnerability must not be installed or used. Excepted from this rule are components for which the vendor has already provided a measure to remedy the vulnerability, e.g. a patch, update or workaround. In this case, the additional measure must be implemented on the system. Vulnerability management is a permanent process during complete life cycle of the system to fix upcoming vulnerabilities promptly.

*Motivation: Publication of vulnerabilities increases the risk of successful exploitation by an attacker. The likelihood raises because of publication of detailed information and tools that help to exploit the vulnerability.*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Disruption of availability

ID: 3.01-6/3.0

# 10. Authentication parameter password

| | |
|---|---|
| Req 32 | If passwords are used as an authentication attribute, those must be stored using a suitable and approved "Password Hashing" method to protect against offline-attacks like brute force or dictionary attacks. |

If an attacker takes possession of a copy of the system user database, he will be able to bring it to a fully independent environment and utilize automatized dictionary or brute force attacks to determine contained passwords. Specialized tools in combination with high computing power allow for high cracking rates in a relatively short period of time, if protective measures are insufficient. Due to the independency from the source system, such an offline attack happens unnoticed.

**The following countermeasure must be implemented, since this ensures best possible protection against offline attacks**

- passwords must be stored using a cryptographic one-way function ("Password Hashing") which is suitable for that purpose and verifiably secure as matters stand

*Please Note: valid password hashing algorithms are described in Security Requirement Catalog "3.50 Cryptographic Algorithms and Security Protocols".*

**Explicitly NOT PERMISSIBLE is**

- to store passwords in cleartext
- to store passwords in any format which can be directly backcalculated

*Please Note: In this context, "directly backcalculatable formats" refers to those that simply encode the password, without involving a secret key in the transformation process. Since the password will no longer show up as original cleartext after it has been processed, those formats may easily be mistaken to provide confidentiality. Effectively, they do not offer any protection. The enconding is fixed and therefore an attacker can easily make use of it to compute the original cleartext password from the encoded string.*
*Examples for directly backcalculatable formats are: "base64", "rot13"*

*Motivation: Without protective measures, an attacker in possession of a user database copy is able to determine masses of contained passwords in short time by merely trying out character string combinations or making use of dictionaries. Passwords stored in cleartext or any backcalculatable format are fully defenseless to an offline attack. Once a password has been ascertained it can be used by an attacker for unauthorized access to the system and the data on it.*

For this requirement the following threats are relevant:

- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 3.01-26/3.0

# 11. Logging

| Req 33 | The system clock must be synchronized to a accurate reference time (Time Standard). |
|---|---|

A time reference source must be used which provides a time signal based on the Coordinated Universal Time ("UTC" = "**U**niversal **T**ime **C**oordinated").

*Please Note: The UTC-synchronized system time may be transformed to local time using a corresponding timezone configuration setup for any output of time information, as long as this timezone adjustment is fully accountable.*

Systems belonging to the same security domain must synchronize to one and the same time reference source.

*Motivation: Reference time synchronization may be a technical prerequisite for many time-dependent mechanisms, for example: Validation of Certificates; Authentication. It is also much-needed to generate exact timestamps for logged events, since without the often required time-related correlation in case of a Security Incident or during a Problem Analysis cannot be achieved.*

Implementation example: some valid time reference sources:

- trustworthy NTP ("**N**etwork**T**ime**P**rotocol") Server on the IP network
- DCF77 radio signal received via a physical attached receiver
- GPS radio signal received via a physical attached receiver

For this requirement the following threats are relevant:
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 3.01-28/3.0