3.2.2 Authenticating the identity of organizations

A basic requirement for being able to use SBCA is to set up a master domain within the **Error! Unknown document property name.** PKI service. The technical configuration of the PKI client is based on the filled-in request for the setup of a master domain. For proper identification purposes and, consequently, to prove the existence of the organization, T-Systems requires an official and current document (e.g., certified copy of the extract from the commercial register or similar document) which must not be older than 30 calendar days. In the case of authorities, the official seal and signature of a person authorized to act on behalf of the authority are sufficient for this request.

T-Systems makes sure that the name of the master domain exists only once. The master domain is generally named after the client's/customer's domain name (second level domain, third level domain). This is also permanently entered into each certificate of the "Organizational Unit Name 1" (OU1) client/customer attribute (see Section **Error! Reference source not found.**).
If the domain name cannot be used to create the name (e.g., only one DNS name is registered for the customer, but multiple master domains are required from a technical perspective), another name may be issued. However, names which allow the client to be traced are to be preferred.

Upon authentication, T-Systems ensures that names that suggest authorizations which the subscriber does not have are not used. Furthermore, slogans or names with racist or pornographic connotations or names suspected of falsely assuming or concealing the identities of organizations are prohibited.

Checking the request for the setup of a master domain also involves checking the customer's/client's identity. In the event that a third party requests a master domain on behalf of the client/customer, additional written authority of the latter is required. Written authority is also required if a third party manages the certificate on behalf of the client/customer. This written authority is issued by the client/customer for the third party.

T-Systems performs the following checks:

- Verifying the organization's existence through a third party ID checking service/database or through the relevant current organizational documents which were issued by or submitted to a competent office/authority and which confirm the organization's existence (e.g., extract from commercial register or similar document which must not be older than 30 days, official seal)
- Checking the domain name(s) against publicly accessible databases (e.g., WhoIs query via Denic eG)
- Verifying the existence of the responsible contact as specified in the "Request for master domain setup" document, who has been identified as the master registrar. Furthermore, checks must be carried out to determine whether the person specified does work for the organization (client) or has been given authority to act on behalf of the organization

- Additional checks as required (e.g., to meet the U.S. American export provisions and licenses of the United States Bureau of Industry and Science (BIS)).

To verify the existence or address of the organization, other methods may be used as an alternative/in addition to the commercial register or comparable directories. If required, a Dun & Bradstreet report can be used as a trustworthy, reliable and independent source of data.
Another method permitted for verification is the submission of a legal statement issued by someone with the relevant qualification. Also, an employee of the registration authority or someone acting on its behalf may personally visit and confirm the specified location.

When setting up the master domain, only those domains for which the client is able to provide the relevant proof (e.g., Denic) will be used for the server, router/gateway and domain controller certificates. The domain names are valid for the entire master domain and are also passed on to areas of responsibility (sub-domains).

If it is a DNS name, the name of the master domain(s) is also included in the master domain configuration (PKI client, external registration authority) as a "permitted Internet domain." Other "permitted Internet domains" can be included for the master domain (PKI client, external registration authority) if a check of equal value to the master domain name check is carried out. If the "permitted Internet domain" is not registered to the master domain owner, an authorization document is required (see Section **4.2.1.1**).

The master registrar certificate issued by the Trust Center operator to manage the master domain contains a unique name (Common Name) for the PKI system.
Suitable and verifiable identification documents which clearly indicate the change request (e.g., master registrar, organization) are required to issue additional master registrar certificates, change configuration in the master domain or revoke master registrar certificates.

The successful identity check of the organization results in the issue of a master registrar certificate, in the name of the master registrar who acts as the top registration authority within the master domain (Section **Error! Reference source not found.**). To ensure the highest level of security, master registrar certificates are always issued on smartcards. If master registrar certifications have become invalid or are revoked, a new request with the relevant ID check must be made.

Organizational changes (e.g., change of company name) or appointment of a new master registrar must be notified to the publisher (see Section **Error! Reference source not found.**) of this Certificate Policy (CP) / Certification Practice Statement (CPS) without undue delay in writing. T-Systems reserves the right to revoke the master and subregistrar certificate(s) (including their derivatives) without delay in the event of the revocation reasons listed in Section **Error! Reference source not found.**.

Additional checks are carried out as required.

To fulfill and comply with the [CAB-BR], T-Systems will repeat the process of authenticating the relevant organization's identity after 39 months at the latest. T-Systems

reserves the right to request current identification documents of the master domain's owner and/or a third party at that person's expense.

3.2.3 Authenticating the identity of end users

The identity or identification of end users (see Section **Error! Reference source not found.**) is authenticated by the registration authority set up at the client (see Section **Error! Reference source not found.** et seq.).
The following registration methods are available for SBCA as standard:

- Central registration (central registration model), i.e., following successful registration of the end user, the subregistrar requests the certificate from the subregistrar website (using a web form or in bulk) and directly receives this certificate or the key material for the end user (excluding the registrar certificate)
- Local registration (central registration model), i.e., the user requests the certificate from the user website or by sending an e-mail request, or the device uses its SCEP interface to request the certificate which is processed by the subregistrar (approval, denial or deferral (resubmission))

Please refer to the "Service Specifications for **Error! Unknown document property name.**" for a more detailed description of the two registration models.

The relevant registration processes are described in the respective manual. The following guidelines apply:

- An end user is always registered via the responsible subregistrar. An exception is the automated bulk generation of key material.
- The subregistrar decides whether the certification request is approved, denied or deferred (resubmitted).
- A renewal function which can be used any number of times, provided that the certificate data (e.g., organization) does not change, is available for user certificates. It is up to the client to decide whether this renewal function may be used in principle. No renewal function is available for device certificates.

3.2.3.1 Registration of a master registrar

The master registrar is registered by T-Systems as part of the identity check of an organization (see Section 3.2.2).

3.2.3.2 Registration of a subregistrar

The client can arrange for one ore more areas of responsibility (sub-domains) to be administrated by subregistrars. The following rules apply:

- The client's master registrar registers a subregistrar and issues the subregistrar certificate.
- The registration is issued to the subregistrar in person or on the basis of a client database with integrity.

The same procedure also applies to subregistrar derivatives (see Section **Error! Reference source not found.**) which are required for the optional "Central key backup" feature in order to download P12 and password files.

3.2.3.3 User registration

Users (natural person, groups of persons/functions, pseudonym, legal person) are registered centrally or locally by the subregistrar. The guidelines described in Section **4.2.1.2** apply.

3.2.3.4 Device registration

Devices (server, router/gateway, mail gateway and domain controller) are registered centrally or locally by the subregistrar. The guidelines described in Section **4.2.1.2** apply.

3.2.5 Checking the authorization

3.2.5.1 Ensuring the authenticity of the certification request

Every customer (client) signs a contract on the "**Error! Unknown document property name.**" PKI service with T-Systems. The customer provides T-Systems with the name of an employee who takes on the role of master registrar. The customer also names the employees who take on the role of subregistrar (derivatives of the subregistrar, where appropriate).

To verify the authenticity of the named master registrars, a call is made to the customer's central telephone number which is stored in the commercial register or a comparable directory. The T-Systems registration authority employee performing this (TC Operator) asks the switchboard to be connected to the aforementioned representative of the customer and thus confirms the authenticity of this person.

3.2.5.2 Checking domains and IP addresses

The customer notifies T-Systems of the domains for which certificates are to be issued so that T-Systems can check them, include them in the client's PKI configuration as "permitted Internet domains" and maintain them. Changes to these domains must be notified to T-Systems in writing.

The T-Systems registration authority employee checks for each entry whether the customer (client) has the legitimate right to use the relevant domain. This involves querying the online database of the country-specific NIC unit (e.g., Denic eG for Germany) for geographic ccTLDs or the online database of the WhoIs for gTLDs. To check an IP address, adequate online databases are queried.

If this does not lead to a successful result, it is checked whether the client/customer has been authorized by the applicant to use the domain or IP address. The applicant is the user or representative of an organization, who controls or operates the device listed on the certificate, even if the device sends the actual certification request. The written authorization must be issued by the user, domain owner or admin C of the device.

To fulfill and comply with the [CAB-BR], T-Systems will repeat the process of authenticating the relevant organization's identity after 39 months at the latest. T-Systems reserves the right to request current identification documents of the master domain's owner and/or a third party at that person's expense.

3.2.5.3 Additional checks by the client

If the certification request shows that the name of a natural person is linked to the name of an organization in such a way that it becomes clear that the person is able to act on behalf of this organization, the client's registration authority

- will check whether the organization exists. This involves using a third party ID checking service/database or requesting documents from the government/authority responsible which confirms the existence of the organization, and
- obtaining business information which confirms whether the person requesting the certificate is employed by the organization and, if necessary, whether the person is authorized to act on behalf of the organization

---

4.2 Processing certification requests

4.2.1 Performing identification and authentication

4.2.1.1 Internal registration authority

The issue of the master registrar certificate is based on the successful authentication of the identity of organizations. This is described in Section **3.2.3**.

4.2.1.2 External registration authority

End users are authenticated by subregistrars (see Section **Error! Reference source not found.** et seq.) within the registration authority responsible, which has been set up at the client.

The external registration authority undertakes to perform the following tasks:

- Registration is performed through
  - personal appearance of the end user, his deputy or a key owner who has authenticated himself by presenting appropriate ID documents and who is responsible for the proper preparation of the certification request and the certificate installation, or

    - another appropriate process (e.g., request via the user website, e-mail or SCEP interface), which clearly indicates the end user's identity. The subject data of the certificate may be based on a client database with integrity.
- Where certificates are requested for devices or groups of persons/functions, the natural person (e.g., administrator) who controls or operates the device listed in the certificate must be authenticated as well.
- The registration authority employee accepts the electronic or paper-based certification request, verifies its integrity and authenticity and checks the details it contains against unique identification documents presented by the applicant (e.g., company ID, personal ID, ERP system) for authenticity (whether they are genuine and trustworthy), integrity (whether they have not been tampered with), correctness, truth and completeness. Reliable internal and public data sources may be used to authenticate the request data.
- In the case of user certificates which will be used for e-mail security (S/MIME certificates) and which are issued by the "Shared Business CA 3" or "TeleSec Business CA 1" sub-CA, the external registration authority must perform an electronic check of the e-mail address. This is done on the basis of a challenge response procedure where the end user is requested proactively to verify the existence of the e-mail address.
- If the certificate is requested electronically via the relevant website or e-mail interface, the domain part of the e-mail address (optionally also the UPN) is checked for the "permitted Internet domains" entered in the PKI configuration.
- In the case of device certificates, the domain part of the e-mail address or the DNS name (top level domain and other FQDN sub-domains) is to be checked for the "permitted Internet domains" entered in the PKI configuration, depending on the certificate type.
- If the client has additional domains for which the certificates are to be issued, T-Systems must be notified of the additional domains. Following a successful domain check, these will be included in the PKI configuration of the master domain (PKI client) (see also Sections **3.2.2** and 4.2.1.1).
- Applicants providing misleading request details are to be rejected.
- If the names are identical, the registration authority must render them unique.
- If the request data does not match the client data (country name (C), organization name (O), organizational unit name, domain part of the e-mail address and, if necessary, user principal name (UPN), top level and other sub-domains of the fully qualified domain name (FQDN), see also Section **Error! Reference source not found.**), the applicant must submit an authorization document.
- In the case of certificates for group/functions or pseudonyms, the information provided in Section **Error! Reference source not found.** applies.
    - For group/function certificates, the real identity of the applicant responsible or his deputy must be checked and assessed by the subregistrar, and then documented following approval.
    - If a pseudonym is used, the official identity of the end user or certificate holder must be checked, assessed and documented by the subregistrar.
    - This is the client's responsibility.
- Copies of the unique ID documents presented by the applicant must be archived for at least 7 years at the expense of the client/external registration authority in a

tamper-proof manner. This archive must be adequately protected against admittance and access.

- In the case of audits or other reviews (e.g., random checks), the registration documents must be disclosed to T-Systems or a qualified auditor appointed by T-Systems.
- Depending on the registration model (Section **3.2.3**), a check must be carried out to establish whether the applicant or deputy accepts the subscriber agreement and/or terms of use. If acceptance of any of these documents is refused, the entire certification request must be denied.
- Where server certificates are issued by the "Shared Business CA 3" or "TeleSec Business CA 1" sub-CAs, the registration authority employees must meet the provisions in the relevant current version of the [CAB-BR], see Sections 9.2.4 and 11.2.
- The registration authority employees are obliged to report any suspicions of compromised keys, certificate misuse or other (attempted) fraud in relation to certificates to T-Systems.
- Certification requests, whose entries match those in the "Denied List" must also be approved by the T-Systems Trust Center.
- Certification requests whose entries match those in the "High Risk List" must be checked by the registration authority employee with particular care.

4.2.2 Approving or denying certification requests

4.2.2.1 Internal registration authority

To validate a request, T-Systems only uses documents, documentation or other information not older than 39 months at the time the certificate is issued.

If the authentication of the required end user information according to Sections **3.2.2** and 4.2.1.1 has been successful, the certification request is approved and the master registrar certificate issued.

4.2.2.2 External registration authority

Only after the subscriber has registered successfully will a certification request be processed further (see Sections **3.2.3** and 4.2.1.2). Depending on the registration model (see Section **3.2.3**), the subregistrar enters the certification request electronically via his website or approves the request which has already been submitted electronically.
If the submitted identification documents are incomplete, untrue or incorrect, the certification request must be denied in an appropriate manner (e.g., by e-mail or phone), specifying the reasons.
If the identification documents are incomplete, the registration authority employee may apply for resubmission.

If the certification request is made via the websites, it is checked for increased risk resulting from entries in the following lists:

- **Denied List:** T-Systems maintains an internal database containing certificates which have been revoked in connection with phishing, misuse or fraud attempts.

This information is used to be able to identify future suspicious certification requests.

- **High Risk List:** T-Systems maintains a database containing organizations as well as domain names or IP addresses which may become a target of phishing, misuse or fraud attacks due to their attractiveness. These certification requests are identified automatically to notify the registration authority employees to take particular care. A documented process is followed here. This is to generate additional vigilance and attentiveness when checking request data. In individual cases, the verification process can have the effect that a requested certificate is not issued.

If the certification request matches entries in the "Denied List," additional approval is required from the T-Systems Trust Center.
If the certification request matches entries in the "High Risk List," the applicant is notified that he is in the process of requesting a certificate which meets the "High Risk Criteria" and that the registration authority employee is to perform the registration process with particular care. In addition, this verification is to be confirmed in the electronic request in writing.