Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programme of Requirements part 2: Admittance to and Supervision within the PKI for the government

Version	4.10
Date	March 1, 2022

Publishers imprint

Version number	4.10
Contact person	Policy Authority of PKIoverheid

Organization	Logius

Street address
Wilhelmina van Pruisenweg 52

Postal address
Postbus 96810
2509 JE DEN HAAG

T 0900-555 4555
servicecentrum@logius.nl

Contents

Policy Authority

The Policy Authority (PA) of the PKI for the government (PKIoverheid) supports the Minister of the Interior and Kingdom Relations in the management of the PKI for the government.

The government's PKI is an trust framework. This system enables generic and large-scale use of the electronic signature and it also facilitates remote identification and confidential communication.

The tasks of the PA of PKIoverheid are:

- contributing towards the development and the maintenance of the framework of standards that underlies the government's PKI, the Programme of Requirements (PoR);
- supervising and preparing for the process of admittance of Trust Service Providers (TSPs) to the government's PKI;
- regulating and monitoring the activities of TSPs that issue certificates under the root of the government's PKI.

The purpose of the Policy Authority is:

Enforcement of a practicable and trustworthy framework of standards for PKI services that provides an established level of security for the government's communication needs and is transparent to users.

1 Introduction

1.1 Background

This is part 2 of the Programme of Requirements (PoR) for the PKI for the government. Set out in the PoR are the standards for the PKI for the government. This part concerns the Trust Service Provider (TSP) joining the PKI for the government and the PAs supervision of TSPs that have joined the PKI for the government.

For a detailed explanation regarding the background and structure of the PKI for the government please refer to part 1 of the Programme of Requirements. This also covers the cohesion between the various parts of the Programme of Requirements.

1.2 The aim of this document

Within the PKI for the government, certificates are issued by TSPs to end users. To be able to issue PKIoverheid certificates, a TSP has to be incorporated into the hierarchy of the PKI for the government. More specifically, this means that the public key of a TSP has to be signed by a Domain CA of the PKI for the government.

To safeguard the trustworthiness of the PKI for the government, TSPs within the PKI for the government have to be reliable organizations that fulfil high requirements in respect of their operational procedures, technical devices, security of information, expertise and reliability of staff and the provision of information to their audience. The specific requirements which a TSP has to fulfil in order to be able to issue certificates within the PKI for the government are listed in part 3 of the PoR.

TSPs that wish to join the PKI for the government have to demonstrate that they fulfil the requirements laid down in part 3. To specify how a TSP has to demonstrate compliance with the requirements that have been laid down and how the admittance process works, this document describes in detail the admittance process and the associated formalities.

To safeguard the trustworthiness of the PKI for the government in an enduring manner, the TSPs have to continue to fulfil the requirements stipulated in part 3 after their admittance to the PKI for the government. To ascertain this, the Policy Authority PKIoverheid (PA) supervises the TSPs that have joined. Therefore, this document also provides an insight into how the PA regulates and which formalities the TSP has to meet to regularly demonstrate compliance with the stipulated requirements.

When compiling this document, where possible use is made of generally accepted standards and certification schemes.

1.3 Status

This is version 4.8 of part 2 of the Programme of Requirements. The current version has been updated up to February 3, 2020, inclusive.

1.4 The structure of this document

Chapter 2 provides a description of the admittance process to the PKI for the government. Successively this chapter deals with the applicable requirements, certification and the approved audit declaration, and the admittance process.

Chapter 3 details the supervision of TSPs within the PKI for the government. It outlines which documents have to be submitted periodically and the applicable schedule.

1.5 Standards and legislation

The standards and legislation referenced in this document [no.], are included in part 1 under paragraph 1.5 of the PoR.

2 Joining the PKI for the government

2.1 Requirements relating to TSP services

Part 3 of the PoR lists the requirements which the TSP services have to fulfil when a TSP wishes to join the PKI for the government. Part 3 is also the so-called Certificate Policy (CP) that applies to the certificates issued by the TSP. In part 3, a distinction is made between the following categories of requirements:

- *TSP services*
  This category of requirements is the main part of part 3. The requirements are made up of:

1. the requirements that are laid down in the Trust Services Decree and the European regulation 910/2014 (eIDAS);
2. ETSI EN 319 411-2 (specifically for the qualified certificates);
3. ETSI EN 319 411-1 (specifically for non-qualified, server, website and EV SSL certificates);
4. Additional PKIoverheid requirements (hereinafter: PKIo requirements);
5. CA/Browser Forum: "Network and Certificate System Security Requirements" (Netsec).

- *Certificate profiles and certificate status information*
  The requirements in this category relate to the content of the certificates to be issued and the format in which the certificate status information (for example a Certification Revocation List or the Online Certificate Status Protocol) are presented. The requirements are divided into legal requirements, requirements under ETSI and additional PKIoverheid requirements. This category of requirements is included in part 3 as an appendix to the CP and as such forms part of the CP.

In PoR part 3, the applicable requirements are examined in detail. In this part, among other things, a list is presented which shows how the legal requirements, requirements under the ETSI and the PKIo requirements relate to one another.

2.2 Demonstrate compliance with TSP service requirements

2.2.1 General

In order to establish whether the services of the TSP meet the stipulated requirements, the Policy Authority PKIoverheid requires that:

1. If the TSP wishes to issue non-qualified, server and/or website certificates within PKIoverheid, it has to be certified against ETSI EN 319 411-1, in accordance with the ETSI EN 319 403 scheme. See the appropriate PoR part for the application of specific policy identifiers.

2. by means of an unqualified audit opinion, the TSP demonstrates that it fulfils the PKIo requirements and the requirements from regulation 910/2014 (eIDAS). An unqualified audit opinion is required, as certification schemes do not exist for testing against the PKIo and legal requirements;

3. only in the case of PKIoverheid EV SSL certificates, contrary to the provisions under 2.2.1-1, the TSP may undergo a WebTrust for Certification Authorities – Extended Validation audit.

If the TSP wishes to issue qualified certificates within PKIoverheid the following additional requirements are applicable:

1. the TSP is certified against ETSI EN 319 411-2 in accordance with the ETSI EN 319 403 scheme. This demonstrates that the TSP satisfies ETSI EN 319 411-2. In addition, the report has to state that the TSP fulfils the additional requirements under the eIDAS Regulation.

2. the TSP is registered with AT. The CA with which the TSP wishes to issue qualified certificates must be exist on the TSL with AT before the issuance of qualified certificates can commenced.

In order to be able to determine whether the services of the TSP meet the set requirements, they must provide proof of conformity to the PA. Part 3 of the CP (PvE or program of requirements) describes more about this. The costs for the certification process, the audit statement and the registration with the Dutch supervisor Agentschap Telecom (AT) are entirely borne by the acceding TSP. The following sections deal in detail with the specific requirements and circumstances that apply to obtaining the ETSI certification and the audit statement. For more information about registration with the AT, we kindly refer you to www.agentschaptelecom.nl[1].

What is the ETSI EN 319 403 *scheme?*

The scheme provides and describes the process requirements for:

- the implementation by the Certification Body (CB) of an initial certification audit of the TSP;
- issuing a compliance certificate to the TSP when the requirements of the standard have been fulfilled; the certificate is valid for three years;
- performing an annual verification audit ;
- after two years, performing a reassessment of the TSP; the reassessment carries equal weight to the initial certification audit.
- Due to the additional demands by browser parties the above requirements have been increased by PKIoverheid. An acceded TSP must undergo a full audit annually (see 3.2 as well).

The ETSI EN 319 403 scheme also provides sub-certification. In sub-certification, an organization is certified against a predetermined sub-set of ETSI requirements. This applies when the TSP has, for example, contracted out the certificate generation service. However, the TSP remains ultimately responsible for all aspects of the services. Within the PKI for the government, a TSP is allowed to contract out a part of the services to a different organization. However, the TSP has to provide proof of conformity concerning the services as a whole, including the services that have been contracted out. For further information regarding sub-certification, reference is made to the ETSI EN 319 403 scheme.

Who can certify?

Compliance certification under ETSI EN 319 403 is based on the assessment of the TSP by a CB against the applicable standard, ETSI EN 319 411-2 and ETSI EN 319 411-1. To this end, the CB has to be accredited by the Dutch Accreditation Council or another accreditation body under article 4 of directive (EG) nr. 765/2008. The following paragraph examines the accreditation of a CB in more detail.

Accreditation of a Certification Body

The ETSI EN 319 403 scheme for certification of TSPs lays down the requirement that Certification Bodies have to have been accredited by the Accreditation Council (RvA) or another accreditation body to test compliance with standard ISO 17065. This is the compulsory standard under ISO when certifying products and services. The term of validity of an accreditation is four years. To determine whether, during the period of 4 years, the CB fulfils the standard ISO 17065, the Accreditation Council performs annual audits of the CB. After four years, the CB has to be reaccredited.

1 http://www.agentschaptelecom.nl

It is expected that accredited Certification Bodies perform certification in a trustworthy and professional manner. To guarantee this, requirements are laid down in the ETSI EN 319 403 scheme which the CB and specifically the audit team and the team members have to fulfil. Within the PKI for the government, no additional quality requirements are laid down for Certification Bodies.

2.2.2 Unqualified audit opinion for PKIo requirements - PKI for the government

As outlined in paragraph 2.2.1, the TSP has to have an unqualified audit opinion to demonstrate that the PKIo requirements are fulfilled. As there is no certification scheme for the PKIo requirements, a CB can logically not be accredited by the Accreditation Council to test and certify against the PKIo requirements. To be able to issue an unqualified audit opinion concerning the PKIo requirements, a CB must, however, fulfil the same quality requirements as those stipulated for ETSI EN 319 403 certification. The depth and the method of execution of the audit for this unqualified audit opinion have to be comparable to those of the certification investigation for the ETSI EN 319 403 certification. In part 3 of the PoR, the PKIo requirements can be recognized by the marking [PKIo]. A TSP that issues certificates under a specific domain must comply with the PKIoverheid requirements of the domain in question.

2.2.3 Expansion of the TSP services to issue services certificates and/or autonomous device certificates and/or EV SSL certificates

Deviating requirements

For the issuance of services certificates and/or autonomous device certificates and/or EV SSL certificates, other requirements apply than for the issuance of personal PKIoverheid certificates. The specific requirements laid down for the TSP wishing to issue services certificates are defined in the 'Services' Certificate Policy, which is incorporated in part 3b of the PoR. The specific requirements laid down for the TSP wishing to issue autonomous certificates are defined in the 'Autonomous Devices' Certificate Policy, which is incorporated in part 3d of the PoR. The specific requirements laid down for the TSP wishing to issue EV SSL certificates are defined in the 'Extended Validation' Certificate Policy, which is incorporated in part 3e of the PoR.

2.3 Admittance process

The entire admittance process consists of three phases:

- *Phase 1: Preparation*
  In this phase, the TSP prepares to join the PKI for the government. The TSP organizes its services in accordance with the requirements laid down by the PKI for the government. Furthermore, coordination will take place between the TSP and the PA during this phase.

- *Phase 2: Request for admittance and decision-making*
  This phase ends with a decision made by the Minister of the Interior and Kingdom Relations.

- *Phase 3: Implementation of admittance*
  During this phase, the technical and organizational measures are taken by means of which the admittance will be implemented.

In the following paragraphs, the relevant points of attention are discussed per phase.

2.3.1 Phase 1: Preparation

When the TSP intends to join the PKI for the government, it is recommended that the PA is contacted. It can then be decided to introduce frequent consultations during which coordination takes place between the TSP and the PA. In addition, specific contact persons will be appointed at the TSP and the

PA, to ensure that the lines of communication are transparent and clear. The PA is available during the preparatory phase for any questions relating to the requirements laid down in the PoR and the course of the admittance.

During the preparatory phase, the TSP also has to become familiar with either the agreement or the contract that will be entered into with the Ministry of the Interior and Kingdom Relations. The agreement or the contract will be signed by the TSP, before the Minister of the Interior and Kingdom Relations will made a decision regarding admittance. The standard agreement and/or the standard contract can be requested from the PA.

The aforementioned difference between the ETSI requirements on the one hand and the legal requirements and PKIo requirements on the other hand entails that a TSP can simultaneously follow the certification process for ETSI EN 319 411-2, for ETSI EN 319 411-1 if applicable, and the assessment process for the other applicable requirements within the PKI for the government. Within the same investigation the CB can determine the compliance with ETSI EN 319 411-2, ETSI EN 319 411-1 if applicable, and the legal requirements and the PKIo requirements of the PKI for the government. This can be beneficial to the TSP both in terms of time and money.

The lead time of the first phase very much depends on the situation with the TSP and therefore no estimate can be given.

2.3.2 Phase 2 : Request for admittance and decision-making by the Minister of the Interior and Kingdom Relations

The "Aanvraagformulier toetreding PKI voor de overhead (Application form to join the PKI for the government)" (PKI00112) has to be used to request admittance. This form can be found at https://www.logius.nl/ondersteuning/pkioverheid/aansluiten-als-tsp/ under "Modelcontracten en –formulieren (Model contracts and forms)" and it can also be obtained from the PA. The TSP that wishes to join the PKI for the government has to complete the form and return this to the PA along with supporting documentation. (The address of the PA is given on the application form).

Documentation required with an admittance request

The diagram below shows which documentation has to be provided.

It also outlines which additional documents have to be provided if the joining TSP also wishes to issue services certificates and/or autonomous devices and/or EV SSL certificates.

For Qualified certificates

Document	Explanation
Proof of registration with the AT.	This demonstrates that the TSP is entitled to issue qualified certificates to the public. If the TSP has a branch in the Netherlands, the TSP has to be registered with the Agentschap Telecom (AT) or alternatively, if the TSP does not have a branch in the Netherlands, with a different national entity appointed by a member state of the EC, that fulfils a similar function to AT.

Document	Explanation
ETSI EN 319 411-2 certificate (including full report of the certification)[1].	The PA wishes to receive the report in order to gain insight into any potential non-conformities. The report has to state against which version of the requirements document an assessment has been made.
Unqualified audit opinion for the PKIo requirements of the PKI for the government (including full report)[2].	This opinion demonstrates that the TSP fulfils the PKIo requirements. The PA wishes to receive the report in order to gain insight into any potential non-compliances. The report has to state against which version of the requirement documents the assessment was made and which published amendments to the PoR applicable at that time have been included.
Certificate profile for end users.	This is the blueprint for the certificates to be issued by the TSP. As in the event of non-compliance any issued certificate has to be revoked, it is advisable that the PA vets this certificate profile beforehand.
Fully completed application form, with the request to join the PKI for the government.	Further details regarding the request are to be included on the form.
Completed OID application form.	Each TSP and CA within the PKI for the government will receive their own OID. Based on the completed application form, the PA requests an OID for the TSP and CA.
Proof that the TSP is authorized to represent an organizational entity.	The PA is responsible for identifying, with certainty, the (representatives of the) TSP.
The signed agreement or contract with the Ministry of the Interior and Kingdom Relations in duplicate.	The Ministry of the Interior and Kingdom Relations is owner of the PKI for the government and therefore a formal agreement or contract has to be entered into with the Ministry of the Interior and Kingdom Relations for admittance to the PKI for the government.

Additional for non-qualified certificates including services certificates and Autonomous devices certificates.

ETSI EN 319 411-1 certificate (including full report of the certification).	The PA wishes to receive the report in order to gain insight into any potential non-conformities. The report has to state against which version of the requirements document an assessment has been made.
Unqualified audit opinion for the PKIo requirements of the PKI for the government (including full report)[1].	This opinion demonstrates that the TSP fulfils the PKIo requirements. The PA wishes to receive the report in order to gain insight into any potential non-compliances. The report has to state against which version of the requirement documents the assessment was made and which published amendments to the PoR applicable at that time have been included.
Certificate profile for non-qualified certificates.	See certificate profile for end users.

Additional for server, website and EV SSL certificates.

Document	Explanation
ETSI EN 319 411-1 certificate (including full report of the certification).	The PA wishes to receive the report in order to gain insight into any potential non-compliances. The report has to state against which version of the requirements document an assessment will be made.
Instead of a ETSI EN 319 411-1 certificate, a declaration from a qualified auditor that there is compliance with the WebTrust for CA Extended Validation criteria.	The PA wishes to receive the report in order to gain insight into any potential non-compliances. The report has to state against which version of the document outlining the requirements the assessment was made.
Unqualified audit opinion that the PKIo requirements of the PKI for the government have been fulfilled (including full report).	This opinion demonstrates that the TSP fulfils the PKIo requirements of CP part 3f EV. The PA wishes to receive the report in order to gain insight into any potential non-compliances. The report has to state against which version of the requirement documents the assessment was made and which published amendments to the PoR applicable at that time have been included.
Certificate profile for EV SSL certificates	See certificate profile for end users.

Decision-making

After receipt of all required documentation, the PA assesses to what extent the request and the documentation that has been provided contain sufficient and adequate information to take the admittance request under consideration. If the admittance request is incomplete or unclear, the PA

will make time for consultation with the TSP. The documentation will be returned to the TSP with the request to modify or to expand on the set of documentation.

If the request is complete and correct, the PA will advise the Minister of the Interior and Kingdom Relations. The Minister of the Interior and Kingdom Relations will then decide whether or not to honour this request for admittance. The Ministry of the Interior and Kingdom Relations will inform the TSP about the Ministers decision. In the event that a positive decision is taken, the Ministry of the Interior and Kingdom Relations will instruct KPN Corporate Market B.V (hereinafter KPN), the technical administrator of the PKI for the government root, to include the TSP in the hierarchy of the PKI for the government.

The completion time of Phase 2 amounts to a few days, unless there is a reason for the PA to consult the TSP. This situation is only foreseen if the request for admittance is incomplete or unclear.

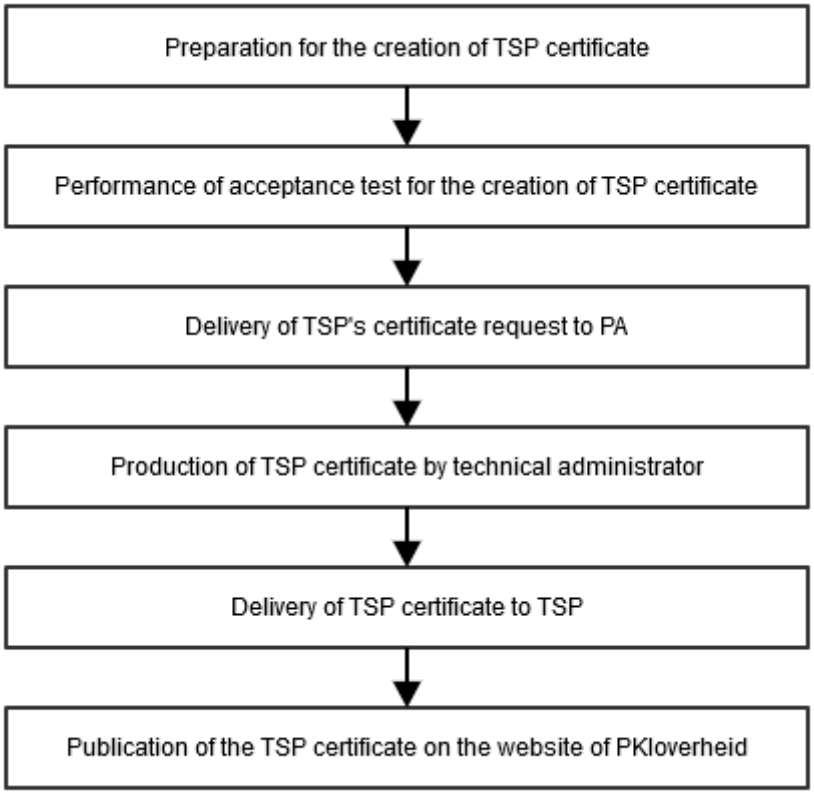
[1] For the aforementioned approved declarations, the CB does not have to be accredited but has to fulfil the stipulated quality requirements (see paragraph 2.2.2).

[1] The ETSI EN 319 403 certificate has to be issued by an accredited Certification Body.

[2] For the aforementioned approved declarations, the CB does not have to be accredited but has to fulfil the stipulated quality requirements (see paragraph 2.2.2).

2.3.3 Phase 3: Implementation

When joining the PKI for the government, the TSP has to have its public key [1] signed by the relevant domain key of the PKI for the government. The signed TSP certificate can only be used to issue certificates and to publish CRLs, in accordance with the Programme of Requirements of the PKI for the government, and to sign the certificates of any sub-CAs. To arrive at a TSP certificate that has been signed by the PKI for the government, a number of process steps have to be followed. These steps are shown as a diagram in the following figure, the steps are then explained.



Preparation for the creation of TSP certificate

During this phase, the TSP is appointed a contact person at the PA. This contact person provides the TSP with the information required for implementation. During the coordination phase, the following sub-steps are followed:

1. *Discuss the technical and organizational preconditions*
   This includes the project planning of the technical certification process, the appointment of anyone who needs to be present and the organization of the ceremony.

2. *Enter into the contract between the TSP and KPN*
   For the acceptance test that is to be performed, the TSP and KPN have to enter into a contract. To this end, the PA provides (amongst other things) the names of the contact persons at KPN and other details (such as a draft date for the key ceremony).

3. *Provision of an OID number*
   The OID number requested by the TSP is sent by the PA to the TSP.

At this time in the procedure, all data, with the exception of the validity data, are included in the naming document. The naming document has to be used for the actual production of the TSP certificate [1] .

Performance of acceptance test for the creation of TSP certificate

The acceptance test is performed as part of this step. This stage comprises the following sub-steps:

1. *Performance of the acceptance test*
   During the acceptance test, the signing script and key ceremony are performed in full as a dry-run (test) for the production phase. The acceptance test is performed jointly by the TSP and KPN, without the involvement of the PA. At the end of the acceptance test, the TSP and KPN perform a technical verification of the test TSP certificate that has been produced.

2. *Verification by PA*
   After performance of the acceptance test, KPN sends the test TSP certificate to the PA. The PA then verifies whether the content in the various fields is correct. A final date is then established for the production.

Delivery of TSPs certificate request to PA

This stage comprises the following sub-steps:

1. *Send request to PA*
   The TSP generates a certificate request (a PKCS#10 file) and securely submits the request, including a print of it, to the PA.

2. *Verification by PA*
   The PA checks the certificate request, to ensure a greater level of guarantee that no problems will arise during production. In addition, KPN has to send the fully completed naming document for verification to the PA. When the verification of the certificate request and of the naming document is positive, the TSP certificate can be produced and the TSP and KPN are informed of this. The PA then securely submits the certificate request to KPN.

Production of TSP certificate by technical administrator

This stage comprises the following sub-steps:

1. *Submission of the certificate request to KPN*
   The PA securely submits the certificate request to KPN.

2. *Generation of the TSP certificate*
   The TSPs public key is physically signed by the signing key (of the relevant domain) of the PKI for the government. The PA is present during this process to establish the accuracy of the process. The TSP is not present when the TSP certificate is generated. The output of this step is a TSP certificate signed by the relevant Domain CA.

Delivery of TSP certificate to TSP

This stage comprises the following sub-steps:

1. *Verification by PA*
   The PA receives the TSP certificate from KPN and checks the TSP certificate. If the check is positive, the PA sends a letter to KPN which states the positive result.

2. *Handover to TSP*
   The PA hands the TSP certificate over to the TSP. The TSP then checks the TSP certificate and signs a confirmation of receipt, in which the content of the TSP certificate is approved. The handover takes place directly after the generation at KPN in Apeldoorn. From that moment onwards, the TSP is responsible for the transport to the location of the TSP certificate and the further processing of the TSP certificate signed by the Domain CA. The transport of the PKCS#7 file to the location of

the TSP has to take place in a way that is comparable to submitting the PKCS#10 file, to ensure a comparable degree of trustworthiness.

Publication of the TSP certificate on the website of PKIoverheid

After submission of the TSP certificate, the PA will publish the TSP certificate on its website http://cert.pkioverheid.nl .

Lead time

The estimated lead time of this implementation of admittance phase is two months. If the TSP lays down specific requirements (detailed key ceremonies, presence / use of several parties) or should unforeseen technical complications arise, the completion time can increase.

Costs

The costs for completing this phase will be borne in full by the joining TSP and amount to € 7,000.00 for one TSP CA. For each additional TSP CA an additional cost of € 1,000.00 per CA will be incurred with a maximum of 6 CAs. If a TSP wishes to have more than 6 TSP CA certificates signed the TSP must contact the PA. This amount is stipulated in the agreement between the Ministry of the Interior and Kingdom Relations with KPN as technical administrator of the root.

[1] Deviations from the naming document can be a hindrance, particularly when fields

marked as 'critical' differ from the required certificate profile.

[1] "Key", "TSP certificate" and "naming document" can also be read as "keys", "TSP certificates" and "naming documents", depending on the design of the CA structure chosen by the TSP

3 Supervision

3.1 Introduction

To permanently safeguard the security of the PKI for the government, the TSPs will have to continue to fulfil the requirements stipulated in part 3 after joining the PKI for the government. To determine this, the Policy Authority PKIoverheid (PA) supervises the TSPs that have joined. This chapter outlines which documents have to be regularly submitted and the applicable schedule.

3.2 Documents to be submitted regularly

In chapter "Admittance to the PKI for the government" paragraph 2.2.2 states that a ETSI EN 319 403 certification is valid for two years and that repeat audits have to be performed annually. Due to the additional demands by browser parties the above requirements have been increased by PKIoverheid and a full audit must be performed annually. This system has been adopted by the PKI for the government in relation to the unqualified audit opinions that have to be submitted.

3.2.1 To be submitted annually

The TSP has to submit the following documents annually[1]:

- Proof of compliance with ETSI EN 319 411-2;
- If applicable, proof of compliance with ETSI EN 319 411-1;
- Instead of compliance with ETSI EN 319 411-1 or ETSI EN 319 403 certification: an unqualified audit opinion concerning WebTrust for Certification Authorities – Extended Validation. Only if a TSP issues PKIoverheid EV SSL certificates;
- Unqualified audit opinion for the PKIo requirements of the PKI for the government;
- Unqualified audit opinion that fulfils the requirements based on ETSI EN 319 411-1 of the CP Services and/or Autonomous Devices and/or EV SSL[2].

The complete and final audit report with detailed findings has be submitted to AT and the PA PKIoverheid as soon as it has been supplied by the auditor. This must occur no later than 3 working days after receipt of the report by the TSP. The Corrective Action Plan (CAP) has to be submitted to AT and the PA as soon as it has been approved by the auditor. Where possible, AT and the PA will also receive the sub-certification of sub-contractors. If a follow-up audit is found to be necessary, AT and the PA PKIoverheid wish to receive the results of this audit.

The documents mentioned above can be submitted in a number of languages according to the following overview:

Document	Dutch	English	Other language
Audit report	Permitted	Permitted	Not permitted
CAP	Permitted	Permitted	Not permitted
Conformity Assessment	Permitted	Mandatory	Not permitted

As soon as the TSP has received the unqualified audit opinion(s) from the CB, the TSP has to immediately send these opinions by post or by e-mail to the Policy Authority PKIoverheid. The opinions and the proof of compliance with ETSI EN 319 411-2, and ETSI EN 319 411-1 if applicable,

must also state against which version of the requirements the documents have been assessed and which published amendments have been included in the PoR applicable at that time.

The aforementioned documents have to be provided by a CB; the same quality criteria apply that were applicable at the time of admittance to the PKI for the government.

[1] The period commences at the time that the agreement with the Ministry of the Interior and Kingdom Relations, but not the agreement for provisional admittance, has been signed by both parties.

[2] Of course this declaration only has to be supplied when the TSP has been admitted to issue services certificates or autonomous device certificates and/or EV SSL certificates.

3.2.2 Publication ETSI EN 319 411-1 and/or 411-2 certificate

The TSP must publish the three year ETSI EN 319 411-1 and/or 411-2 certificate on its website.

3.3 Planning

Due to the fact that the opinions (including WebTrust Certification Authorities – Extended Validation) and the proof of compliance with ETSI EN 319 411-2, and ETSI EN 319 411-1 if applicable, have to be submitted annually, these documents logically have a term of validity of one year. The new documents therefore have to be submitted by the TSP to the PA no later than one year after the previous opinion of the CB and the proof of compliance with ETSI EN 319 411-2, and ETSI EN 319 411-1 if applicable. The TSP is responsible for the timely delivery of the opinions and the proof of compliance with ETSI TS 101 456 and, ETSI EN 319 411-1 if applicable.

3.4 Amendments to certification and AT registration

Because it is possible that the ETSI EN 319 411-1 or ETSI EN 319 411-2 certificate is revoked or suspended or the AT registration is terminated, the TSP is obliged to immediately inform the PA if one of the following situations occurs:

- The ETSI EN 319 411-1 or ETSI EN 319 411-2 certificate is revoked or suspended by the CB;
- The ETSI EN 319 411-1 or ETSI EN 319 411-2 sub-certificate of the organization to which the TSP has contracted out activities is revoked or suspended by the CB;
- There is a negative WebTrust for Certification Authorities – Extended Validation opinion;
- The registration of the TSP is revoked by the AT.

3.5 Enforcement of agreements

Government organizations that operate as a TSP within the PKI for the government have entered into an agreement with the Ministry of the Interior and Kingdom Relations. The other TSPs within the PKI for the government have entered into a contract with the Ministry of the Interior and Kingdom Relations. The agreement and the contract outline how the Ministry of the Interior and Kingdom Relations and the TSP have to act within the PKI for the government. It discussed the continued fulfilment of the stipulated requirements and the options the PA has of enforcing the arrangements. This concerns, amongst other things, the option to have an audit performed of the TSP and the dissolution of the agreement or the contract.

The agreements and contracts have a term of validity of six years. Before the term of validity expires, the PA will contact the TSP to discuss potential renewal of the agreement or the contract.

4 Revisions

4.1 Version 1.0

First version.

4.2 Version 1.0 to 1.2

New

None.

Modifications

None.

Editorial

- Only a few editorial changes have been made but these do not affect the content of the information.

4.3 Version 1.2 to 2.0

New

None.

Modifications

- The following paragraphs have been modified in connection with the introduction of the Autonomous Devices Domain within the PKI for the government:
    - Paragraph 2.1;
    - Paragraph 2.2.1;
    - Paragraph 2.2.4;
    - Paragraph 3.2.1.

Editorial

- Only a few editorial changes have been made but these do not affect the content of the information.

4.4 Version 2.0 to 3.0

New

None.

Modifications

- The following paragraphs have been modified in connection with the introduction of Extended Validation within the PKI for the government:
    - Paragraph 2.1;
    - Paragraph 2.2.1;
    - Paragraph 2.2.3;
    - Paragraph 2.2.4;
    - Paragraph 2.4.2;
    - Paragraph 3.2.1.

Editorial

- Only a few editorial changes have been made but these do not affect the content of the information.

4.5 Version 3.0 to 3.1

New

- Paragraph 3.2.3.

Modifications

- Paragraph 3.2.1.

Editorial

- A number of editorial changes have been made but these do not affect the content of the information.

4.6 Version 3.1 to 3.2

New

None.

Modifications

- Paragraph 1.4;
- Paragraph 2.2.1;
- Paragraph 2.3;
- Paragraph 2.4;
- Paragraph 3.2.1;
- Paragraph 3.2.2;
- Paragraph 3.3;
- Paragraph 3.4.

Editorial

- A number of editorial changes have been made but these do not affect the content of the information.

4.7 Version 3.2 to 3.5

New

None.

Modifications

- Paragraph 2.2.1 (effective date no later than 4 weeks after publication of PoR 3.5);
- Paragraph 3.2.1 (effective date no later than 4 weeks after publication of PoR 3.5).

Editorial

None.

4.8 Version 3.5 to 3.6

New

None.

Modifications

- Certification against ETSI EN 319 411-2 (effective date no later than 4 weeks after publication of PoR 3.6);

Editorial

- References to PKIo-OO, PKIo-Bu, PKIo-Sv etc.

4.9 Version 3.7 to 4.0

New

None.

Modifications

None.

Editorial

- References to ETSI EN 319-411-3.

4.10 Version 4.0 to 4.1

New

None.

Modifications

- Changed the normative reference from ETSI EN 319 411-3 to ETSI TS 102 042.

Editorial

None.

4.11 Version 4.2 to 4.3

New

None.

Modifications

- TTP.NL schema replaced by European scheme ETSI EN 319 403 (per 1-7-2016);
- Changed the normative reference from ETSI TS 102 042 to ETSI EN 319 411-1 (per 1-7-2016).

Editorial

None.

4.12 Version 4.3 to 4.4

New

None.

Modifications

- Altered the scope of allowed Certifying Bodies (CB's) in light of the eIDAS directive (1-2-2017).

Editorial

- Replace CSP (Certification Service Provider) with TSP (Trust Service Provider) as a result of the eIDAS regulation.

4.13 Version 4.4 to 4.5

New

None.

Modifications

- Keeping Netsec normative (adopted as reference in ETSI EN 319 411-1 and now normative in the PoR);
- Modified normative references as a result of the repealing of the Electronic Signatures Act and the modification of a number of acts and the introduction of the eIDAS regulation.

Editorial

None.

4.14 Version 4.5 to 4.7

New

None.

Modifications

- Removal of the obligation to hand over an ETSI EN 319 403 certification.

Editorial

None.

4.15 Version 4.7 to 4.8

New

None.

Modifications

- Updated references and links to guidelines.

Editorial

None.

4.16 Version 4.8 to 4.9

New

None.

Modifications

- Corrected text on ETSI 319 403 in Section 2.2.1.

Editorial

None.

Deletions

None.

4.17 Version 4.9 to 4.10 (part 2)

New

None.

Modifications

None.

Removals

None.

Editorial

None.