Certification Practice Statement (CPS)
Document History and Approval

<table>
<thead>
<tr>
<th>Change Control</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version</strong></td>
<td><strong>Date</strong></td>
<td><strong>Author</strong></td>
</tr>
<tr>
<td>0.8</td>
<td>12/01/2007</td>
<td>R. van Groenigen</td>
</tr>
<tr>
<td>1.0</td>
<td>15/02/2007</td>
<td>R. van Groenigen</td>
</tr>
<tr>
<td>1.1</td>
<td>27/11/2007</td>
<td>D. van Mourik</td>
</tr>
<tr>
<td>1.2</td>
<td>11/05/2011</td>
<td>D. van Mourik</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Document History</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td><strong>Version Approved</strong></td>
<td><strong>Position</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1. **INTRODUCTION**

1.1 **Overview**

This document is KAS BANK’s Certification Practice Statement. It states the practices that KAS BANK employs in providing certification services. This CPS shows the practice of KAS BANK in its PKI environment. The CPS controls the certification process, and includes issuing, managing, using, revoking and renewing certificates.

1.2 **Structure**

The CPS regulates the certificate life cycle and describes the certification process. The structure of this CPS is the following:

1  Introduction  
   1.1  Overview  
   1.2  Structure  
      1.3  Identification  
         1.3.1  Certification Authority  
         1.3.2  Registration Authority/Customer Operator  
         1.3.3  End User  
   1.4  Types of Certificates  
      1.4.1  Personal Certificates  
   1.5  Certificate Use Limitation  
   1.6  Contact details  
2  General provisions  
   2.1  Obligations  
      2.1.1  KAS BANK Obligations  
      2.1.2  Registration Authority/Customer Operator Obligations  
      2.1.3  End User Obligations  
         2.1.3.1  Reliability on signatures  
         2.1.3.2  Reliability on Certificates  
   2.2  Liability  
      2.2.1  Certification Authority liability  
      2.2.2  Registration Authority/Customer Operator liability  
      2.2.3  End User liability  
   2.3  KAS BANK Certificates uses  
   2.4  Interpretation and Enforcement  
      2.4.1  Governing law  
      2.4.2  Dispute resolution procedure  
      2.4.3  Registration fees for certificate’s issuance and renewal  
   2.5  Publication and repository
2.5.1 Publication of CA Information

2.6 Confidentiality and data protection
2.6.1 Confidentiality of digital signature keys
2.6.2 Confidentiality of provision of certification services
2.6.3 Data protection

2.7 Intellectual Property Rights

3 Key management
3.1 General provisions
3.2 CA Key management

4 Certificate revocation and suspension
4.1 Circumstances for Revocation
4.1.1 Revocation effects
4.2 Circumstances for Suspension
4.2.1 Suspension effects and limits
4.3 Suspension and revocation procedure
4.3.1 Active authentication
4.3.2 Reception of suspension/revocation requirements
4.3.3 Decision to suspend/revoke
4.3.4 Suspension/revocation communication and publication

5 Certificate expiration

6 Certification services renewal
6.1 Certificates’ renewal

7 CA termination

8 Security controls
8.1 Internal Security Manual
8.2 Classification and control of assets.
8.3 Staff security
8.4 Physical and environmental security
8.5 System management security
8.6 Business continuity plan
8.7 Incidents
8.8 Compliance

9 Certificates and certificate’s lists characteristics
9.1 Certificate’s characteristics
9.2 Certificate lists

10 Other
10.1 CPS and Certification Practices modification procedures
10.2 Modification publication procedure
10.3 Publication notification procedure
1.3 Identification

This CPS is also available at http://pki.kasbank.com. This document’s object identifier is: 2.16.528.1.1009.1.2.1.b

All customer operators and end users admit that they know this document before requesting KAS BANK any type of certificate. They know as well how the public key systems, on which digital certificates are based, work.

For further information, contact KAS BANK at:

KAS BANK N.V.
Service Desk Client Information Management
Nieuwezijds Voorburgwal 225
1012 RL Amsterdam
The Netherlands
Tel. 0031 557 5888
servicedesk@kasbank.com

1.3.1 Certification Authority

KAS BANK acts as a Certification Authority (CA) relating a certain public key to a specific person or entity through the issuance of a Certificate according to the terms of this CPS and the Certification Policy of each type of certificate.

1.3.2 Registration Authority/Customer Operator

KAS BANK acts as a Registration Authority and checks the applicant’s identity according to the terms of this CPS.

KAS BANK could delegate the identity confirmation to one or several Customer Operators, who will function as Registration Authority. The Registration Authorities will check the end users identity according to the terms of this CPS. The relationship with the Registration Authorities is based on specific provision of services agreements.

1.3.3 End user

The end user will be the individual to whom the Digital Certificate has been issued.

The end users will comply with the terms of this CPS, with the Certification Policy of the Certificate they obtained.

The end users will have to keep to the procedures established for the request of each type of certificate and will have to comply with the terms of this CPS.
1.4  Types of Certificates

1.4.1  Personal Certificates

KAS BANK issues certificates that allow signing electronically and link the subscriber’s identity to his public key. It allows the subscriber to sign electronic documents. The verification of the customer operator/end users identity will be in person and with documents. The customer operator/end user will have to appear before a Registration Authority with a valid identity card.

All data contained in the certificates is registered according to the terms of this CPS, the Certification Policy. The person’s verification will be in person and with documents, according to the intake process of KAS BANK.

All data contained in the certificate is registered in accordance with the applicable official practice according to the concrete Registration Authority and that should be consulted in the corresponding Certification Practices.

1.5  Certificate Use Limitation

The authorized uses of Certificates issued by the Certification Authority can be specified in each type of certificate. The certificate holder is obliged to use the certificates issued by KAS BANK only for purposes where KAS BANK services are involved. Without affecting the use limitations that may be established, it is possible to establish limits in the value of transactions where the certificate can be used, with the same requirements established in this CPS for use limitations.

In any case, a certificate can have either use limitations, limitations in the value of transactions, both limitations, or any of them.

1.6  Contact details

KAS BANK N.V.
Service Desk Client Information Management
Nieuwezijds Voorburgwal 225
1012 RL Amsterdam
The Netherlands
Tel. 0031 557 5888
servicedesk@kasbank.com
2 GENERAL PROVISIONS

2.1 Obligations

2.1.1 KAS BANK Obligations

KAS BANK shall:

- Issue certificates in accordance with the terms and conditions of this CPS, the corresponding Certification Policies and application standards.
- Issue certificates which minimum content is specified in certificate’s current regulations.
- Issue certificates according to the information received.
- Maintain its own private keys under its control by using reliable systems and products to store the keys and make them inaccessible to non-authorized people, avoiding their loss or spreading, so that they guarantee their trustfulness.
- Issue certificates in accordance with the terms and conditions of this CPS, each certificate’s Certification Policies, the corresponding provision of certification services agreement and the Registration Authority agreement.
- Use reliable systems and products protected against any alterations that guarantee the technical and cryptographic security of the certification procedures they support.
- Provide access to the current versions of the CPS and Certification Policies of each type of certificates.
- Offer and maintain the necessary infrastructure for certification services, as well as the necessary physical, procedural and personal security controls for the certification practices.
- Approve or reject certificate applications.
- Provide copies of their own certificates or of any revocation information to anyone wishing to verify a digital signature with reference to those certificates. For this purpose, KAS BANK will publish all necessary information at: http://pki.kasbank.com/crl.asp
- Publish the certificates issued in accordance with the provisions of current regulations with regard to data protection.
- Protect personal details in accordance with current legislation with regard to personal details protection.
- Take the necessary steps to avoid certificate falsifications and guarantee the confidentiality of the information provided during the certificate generation, as well as the handing through a reliable procedure.
- Use reliable systems to store certificates that allow checking their authenticity and preventing non-authorized people from changing the data. These reliable systems allow detecting any change affecting the security conditions.
- Do not store or copy the signatory’s signature data.
- Store by any secure mean all information and documentation related to an issued certificate as well as the Certification Practices Statements in force, during a period of 15 years from the issuance of the certificate onwards in time so that the signatures can be verified. For this purposes, KAS BANK stores in printed and digital format all versions of the CPS already published. All issued certificates are stored in PKCS#7 format (without private key) in order to verify, if necessary, a signature made with any of them.
• Inform the subscribers and Registration Authorities related to KAS BANK about the modifications of this Policy and its Certification Practice Statement.
• Comply with the obligations of this CPS, the privacy protection laws and the current regulations.

2.1.2 Registration Authority and Customer Operator Obligations

The Registration Authority for registering Customer Operators is KAS BANK.
The Registration Authority for registering Customer End Users is the Customer Operator.

The Registration Authority will comply with the following obligations. The Registration Authority shall:
• Identify or authenticate the subscriber, the applicant or the organization that he represents, according to the terms and conditions of this CPS and the specific Certification Practices for each type of certificate, by using any authorized means.
• Formalize the Certificate Issuance contracts with the subscriber under the terms and conditions specified by the Certification Authority.
• Store with a safe method and during a period of a minimum of 10 years the documentation provided in the Certificate issuance procedure and in the Certificate revocation/suspension procedure, under the terms and conditions of this CPS, the Certification Policy of each type of certificate and the Registration Authority Agreement.
• Carry out any other job with the staff required in each case, according to the terms and conditions of this CPS, the Certification Policy of each type of certificate and the Registration Authority Agreement.
• KAS BANK reserves the right to revoke or suspend any of the certificates issued, if it is necessary to protect the certification system security.

2.1.3 End User Obligations

End Users shall:
• Provide the Registration Authority or the Customer Operator with the necessary information to make a correct identification.
• Confirm the accuracy and truthfulness of the information provided.
• Notify any change of the information provided during the validity period of the certificate.
• Request the certificate according to the terms and conditions of the Certification Policy of each type of certificate and to the provision of certification services agreement signed with KAS BANK.
• Understand the terms and conditions of this CPS and the Certification Policies of his certificate, as well as the modifications of them.
• Preserve and make good use of the certificate given in deposit.
• Guard the certificate conscientiously taking all the necessary precautions to avoid its loss, revelation, modification or non-authorized use.
• Not make any alteration to the certificate by any means or any person, except if that alteration is specifically authorized by the legislation.
• Request the certificate suspension or revocation when any suppositions specified on the points of this CPS which refer to certificate suspension or revocation may take place.
• Not reveal the private key or the certificate access code.
• Make sure that all information contained in the certificate is correct and notify KAS BANK of any incorrect information that may have been included and that may not correspond to reality. The subscriber is obliged to immediately inform KAS BANK of any change in the information provided, even if this information –such as domicile or telephone number– was not included in the certificate.
• Immediately inform KAS BANK of any situation that may affect the certificate validity.
• Not distribute or transfer the certificate without the prior consent of KAS BANK, except if it is necessary in accordance with the terms and conditions of this CPS, the Certification Policy of each type of certificate and the provision of certification services agreement signed with KAS BANK.
• Destroy the certificate when KAS BANK may demand it by virtue of its property right, when the certificate may expire or be revoked.
• Make good and correct use of the certificate in accordance with the terms and conditions of this CPS and the Certification Policies of each type of certificate. The subscriber will be liable for an incorrect use of the certificate.
• Comply with any other obligation specified by the legislation, by this CPS or by the Certification Policy of each type of certificate and the provision of certification services agreement signed with KAS BANK.
• Users wishing to trust and use the certificates issued by the Certification Authority shall verify the signatures' validity issued by the subscribers.
• If the users don’t proceed to verify the signatures through the Certificate Revoked List, KAS BANK is not responsible for the use and trustfulness that these users make of these certificates.

2.1.3.1 Reliability on Signatures

Any person has the right to rely on an electronic signature issued through a KAS BANK Certificate. To determine if it is reasonable to rely on the signatures, we should bear in mind the following aspects:
• The operation nature that the signature is intended to guarantee. It won’t be reasonable to rely on a signature issued by an KAS BANK Certificate if that operation is considered to be an incorrect use according to the attached list.
• If the relaying party has taken all the necessary steps to confirm the signature’s reliability and, in particular, if it has verified that the certificate has not expired or has not been revoked or suspended. The expiration shall be stated in the certificate. The possible suspension or revocation of the certificate shall be consulted in the Certificate Revocation List.
• If the relaying party knew or should have known that the signature was in doubt or had been revoked or suspend.
• The policies and procedures related to KAS BANK in connection with the signatures issued through certificates. These policies and procedures are specified in this CPS and in the Certification Practices issued for each type of certificate.
2.1.3.2 Reliability on certificates

Any person has the right to rely on an KAS BANK Certificate. To determine if it is reasonable to rely on the signatures, we should bear in mind the following aspects:

1. All restrictions to which the certificate may be subjected.
2. If the relying party has taken all the necessary steps to confirm the certificate’s reliability, (Certificate Revocation List).
3. The policies and procedures related to KAS BANK in connection with the signatures issued through certificates. These policies and procedures are specified in this CPS and in the Certification Practices issued for each type of certificate.

Users of KAS BANK certification service are obliged to understand and accept the terms and conditions of this CPS and the specific Certification Policies of their certificate, established by contract, in which the provision of certification services is guaranteed.

2.2 Liability

This CPS is only the leading document, when there are no other contracts between KAS BANK and the user of a certificate of KAS BANK N.V. The user can be the end user, or the end users employer, or the organization the end user works for.

2.2.1 Certification Authority Liability

- KAS BANK will only be liable for the damages caused to any person when not complying with its legal obligations derived from the current legislation about electronic signature or when acting negligently while providing certification services.
- KAS BANK will not be liable for the damages derived from or related to the failure to comply with applicants, subscribers or users obligations.
- KAS BANK will not be liable for a negligent or fraudulent use of certificates and keys.
- KAS BANK will not be liable for the damages derived from negligent or fraudulent acts on the part of third-parties with regard to the certificates issued by KAS BANK in favor of a subscriber.
- KAS BANK will not be liable for the inaccuracies of the certificate derived from the information provided by the subscriber, assuming KAS BANK has acted with the maximum diligence.
- KAS BANK will not be liable for the damages derived from the operations in which the use limitations stated in the Certification Policies of each type of certificate have not been fulfilled.
- KAS BANK will not be liable for the delay or for the failure to comply with the obligations stated in this CPS if such delay or failure is due to force majeure cases or any other circumstance not controlled by KAS BANK.
- KAS BANK will not be liable for the content of the electronic documents digitally signed.

Neither KAS BANK nor the Registration Authorities will be liable for the damages caused by the use of their public certification services in these situations.
2.2.2 Registration Authority/ Customer Operator Liability

The Registration Authority will be liable for its obligations stated in this CPS, and will specially assume responsibility for the correct identification and validation of the applicant/subscriber, with the same limitations established in the previous section with regard to KAS BANK.

The Registration Authority will be liable for the damages derived from a negligent or different performance of its obligations stated in this CPS and in the Certification Policies of each type of certificate.

Nevertheless, the Registration Authority will not be liable in any case for the applicant/subscriber’s identity in the event of forgery of documents or any other data provided by him or a third-party that could supplant him.

2.2.3 End User Liability

The end user will be liable for the damages caused by the failure to comply with his obligations stated in this CPS.

The end user will be liable for the performance of the obligations stated in this CPS, in the Certification Policies of each type of certificate and in the current regulations with regard to the provision of certification services.

The end user promises to indemnify KAS BANK for the damages caused by any culpable act of omission for his part, assuming the judicial costs KAS BANK may incur, including the costs for lawyers and attorneys. The end user will indemnify KAS BANK for any damage that it may suffer for the total, partial or faulty performance of his obligations and on the basis of all complaints against KAS BANK made by a third-party related to the subscriber.

The end user will be liable for the damages caused by the failure to comply with his obligations stated in this CPS.

The end user will be liable for the performance of the obligations stated in this CPS, in the Certification Policies of each type of certificate and in the current regulations with regard to the provision of certification services.

The end user will always be liable for the risks derived from the acceptance of a certificate without having read the obligations stated in the CPS and in the Certification Policies of each type of certificate, indemnifying KAS BANK for this.

2.3 KAS BANK Certificates’ uses

An improper use of a certificate is considered to be when it is used to carry out non-authorized operations according to the Certification Practices of each type of certificate, the CPS, and the contracts between KAS BANK and its subscribers.

The products, services, activities or goods which importation, exportation, circulation, holding or production is subjected to the acquisition of an authorization or permission, in which case would be governed by it. The products, services, activities or goods illicitly acquired, made, produced or marketed. In general, anything considered to be out of commerce.
2.4 Interpretation and enforcement

2.4.1 Governing law

This document and the Certification Practices for each type of certificate will be governed by Dutch law, in accordance with which should its content be interpreted.

2.4.2 Dispute resolution procedure

In order to resolve any dispute that may arise in connection to this CPS or with the Certification Practices, the parties will refer to the Dutch Court of Arbitration, resigning any other jurisdiction.

2.4.3 Registration fees for certificate’s issuance and renewal

Each Registration Authority will provide applicants with the current registration fees for certificate’s issuance and renewal. Registration Authorities are able to make special promotions or offers that could modify the fees previously established.

2.5 Publication and repository

2.5.1 Publication of CA Information

The content of this CPS, as well as the content of all published information will be available at: http://pki.kasbank.com. The original documents will be kept in the offices of the Certification Authority.

2.6 Confidentiality and data protection

2.6.1 Confidentiality of digital signature keys

KAS BANK guarantees the confidentiality towards third-parties while generating cryptographic signature private keys that it provides to its clients. Moreover, once the private keys have been generated, the Certification Authority will refrain from storing, copying or preserving any kind of information that may be sufficient to reconstruct the keys.

2.6.2 Confidentiality of provision of certification services

Both the Certification Authority and Registration Authorities will be strictly confidential with regard to the information provided by applicants and subscribers of certificates, as long as the publication or communication of that information to third-parties is not necessary for the correct provision of certification services. KAS BANK will ask applicants and subscribers permission to use the data for other purposes.
2.6.3 Data protection

According to the provisions of the regulations about treatment of personal details, the subscriber and applicant are informed about the existence of an automated file of personal details created by KAS BANK, which aim is to be useful according to the terms and conditions of this CPS. The subscriber / applicant allow the transfer of his personal details contained in that file, as far as necessary to carry out the actions stated in this CPS and in the Certification Practices.

The person responsible or the file promises to make everything he can to avoid the alteration, loss, treatment or non-authorized access to the personal details contained in the file. The personal details contained in the file cannot be used for any other purpose without the prior consent of the subscriber / applicant. The subscriber has the right to access to his personal details and correct or cancel them, in accordance with the terms and conditions of the regulations about treatment of personal details.

2.7 Intellectual property rights

KAS BANK has exclusively all intellectual property rights that may derive from the certification system regulating this CPS. It is therefore forbidden to reproduce, distribute, publicly communicate or transform any element belonging to the Certification Authority without its prior consent. Nevertheless, the consent of KAS BANK is not necessary to reproduce the certificate when the legitimate user may need to use it, in accordance with the certificate’s purpose and the terms and conditions of this CPS, the Certification Policy of each type of certificate and the provision of services agreement signed with KAS BANK.
3  KEY MANAGEMENT

3.1  General provisions

Generally, KAS BANK follows a series of standards when generating the two keys, as a certification service provider. The user can check the certificates by checking the chain of certificates in his application. There should never be an invalid certificate in this chain.

3.2  CA Key Management

Hardware Security Modules were used when generating KAS BANK’s CA keys. The Certification Authority’s keys have been kept in a safe-deposit box of an entity specializing in secure storage. The access to these keys is only allowed to people duly authorized by KAS BANK. There is another security copy of the Certification Authority’s key, divided into two parts, each one stored independently and confidentially in KAS BANK’s offices.
4 CERTIFICATE REVOCATION AND SUSPENSION

The certificate revocation and suspension is used if the certificate is not anymore reliable before its expected expiration date, in accordance with the terms and conditions of this CPS.

4.1 Circumstances for revocation

Certificates should be revoked in the event of the following circumstances:
- Subscriber’s voluntary request.
- Loss or irretrievable damage of the certificate’s software.
- Death of the signatory or of his client, total or partial disability of any of them, representation termination or expiry of the legal entity represented.
- Serious inaccuracies in the data provided by the signatory to obtain the certificate, as well as the circumstances that may do that the data originally included in the certificate do not correspond to reality.
- If the subscriber’s private keys have been threatened, either because of loss, theft, robbery, modification, spreading or revelation of the private keys or due to other circumstances, including the accidental, which may indicate that the keys have been used by other person different from the holder.
- If the Registration Authority, the Certification Authority or the subscriber does not comply with their obligations stated in this CPS.
- Repudiation of the contract as it is stated in section 8 of this CPS.
- If there are reasons to believe that the certification service has been threatened to the extent that the certificate may be unreliable.
- Court’s decision or administrative order.
- Concurrence of other circumstances stated in this CPS or in the corresponding Certification Practices of each type of certificate.
- Regarding Business Certificates, the dismissal of the representative of the legal entity represented is also circumstance for revocation.

4.1.1 Revocation effects

When a certificate is revoked, it looses reliability, provoking the permanent cessation of the certificate’s operational ability according to its uses and, consequently, the cessation of the provision of certification services.

The certificate revocation does not allow the subscriber to use the certificate.

The certificate revocation due to circumstances non-attributable to subscribers will originate the issuance of a new certificate in favor of the subscriber for a period equivalent to the remaining period before the expiration date of the revoked certificate.

The notification to third-parties about a certificate that has been revoked, when the verification of it may be requested, will be a consequence of certificate revocation.
4.2 **Circumstances for suspension**
Currently we are not providing suspension services, but it is stated in this CPS for the future.

4.2.1 **Suspension effects and limits**

When a certificate is suspended, it looses reliability, provoking the permanent cessation of the certificate’s operational ability according to its uses and, consequently, the cessation of provision of certification services. The certificate suspension does not allow the subscriber to use the certificate.

The certificate suspension will finish in the event of any the following circumstances:

- Certification Authority’s decision to revoke the certificate.
- Certification Authority’s decision to lift the certificate suspension, once the revocation inadmissibility is considered.
- End in advance of the revocation procedure.

4.3 **Suspension and revocation procedure**

4.3.1 **Active authentication**

The following people should request the suspension or revocation of the certificate if any of the circumstances previously stated arise:

- The certificate’s subscriber as well as the individual or legal entity represented by him.
- The Registration Authority, with regard to the certificates in which issuance they have participated.
- The legal entity stated in the certificate.

Likewise, suspension or revocation could be requested by any third-party with a legitimate interest if he is aware of any of the following circumstances:

- Loss of the certificate’s software.
- Death of the signatory.
- Total or partial disability.
- Inaccuracies in the certificate.
- If the certificate’s reliability is threatened.
- If the keys are threatened.
- Dismissal of the representative in the cases of business certificates.
- Extinction of the legal entity represented.
- Revocation of the entity’s authorization stated in the certificate in the case of business certificates where the owner has no rights to represent the entity.

The Certification Authority is able to start the certificate suspension/revocation procedure in any of the circumstances previously stated.

The judicial or administrative authority could urge KAS BANK to suspend/revoke the certificate according to the provisions of the Dutch Law on Telecommunications about electronic signatures.
4.3.2 Suspension / revocation requests

Certificate suspension / revocation requests could be addressed to the Service Desk Client Information Management.

4.3.3 Decision to suspend / revoke

Once the revocation request has been received and verified, KAS BANK will start the certificate suspension/revocation process. The Certification Authority is in charge of the decision to suspend / revoke a certificate.

4.3.4 Suspension / revocation communication and publication

KAS BANK will inform the subscriber, by normal delivery, about the decision to revoke a certificate. The Certificate Revocation List (CRL) will also be published. KAS BANK’s Certificate Revocation List is published every 24 hours or every certificate revocation. It is possible to see it at:

http://pki.kasbank.com/crl.asp

The revocation will be valid towards third-parties from the moment of its publication, except if the circumstance for revocation is the cessation of KAS BANK’s provision of certification services. In this case, the certificate will not be valid from that moment onwards.

The information related to the revocation state will be available 24 hours a day, seven days a week. If the system, service or any other factor not controlled by KAS BANK fails, KAS BANK should make all efforts to try fixing the problem so that this information service is not unavailable longer than the period stipulated in this policy.
5 CERTIFICATE EXPIRATION

Certificates will expire at the end of their operational period. After the expiration, the certificate will not be valid, provoking the permanent cessation of the certificate's operational ability according to its uses and, consequently, the cessation of the provision of certification services. The certificate expiration does not allow the subscriber to use the certificate.
6 CERTIFICATION SERVICES RENEWAL

6.1 Certificate Renewal

This procedure is used when a certificate is going to expire and the subscriber desires to continue using a certificate with the same characteristics as the previous one. For this purpose, the Customer Operator will issue a new smartcard and new keys will be generated. This time, the verification measures will be minimal, because the old certificate is still valid and there are no reasons to believe that the information provided has changed or that the certificate is not reliable anymore, except if the subscriber confirms it.

The certificates issued by KAS BANK have a validity period which is stated in the certificate. This period will always comply with current legislation. The renewal of certification services can be requested in the event of circumstances stated in the Certification Policies of each type of certificate. The previous requirements, the way of requiring revocation and the certificate renewal procedure are the ones stated in the Certification Policies of each type of certificate.
7 CA TERMINATION

In order to cause as little harm as possible to subscribers and users of the certification system in case of a hypothetical CA termination, the following measures are established:

- KAS BANK will communicate the termination by sending a registered e-mail addressed to all subscribers whose certificates are in force. The communication aforementioned will be carried out two months in advance before the CA termination.
- KAS BANK will carry out any other obligation established by current legislation.
8 SECURITY CONTROLS

8.1 Internal Security Manual

In order to reinforce the technical, physical, procedural and training staff security, KAS BANK has an Internal Security Manual. This document is part of KAS BANK’s internal documentation, what means that it is confidential.

This security manual will be interpreted as the security policy of KAS BANK’s information. This manual is available to all employees working with information systems.

8.2 Classification and control of assets

KAS BANK does stocktaking of all the hardware available to generate business, and particularly of all computers, printers and communication equipments. The hardware’s brand, model, serial number and other characteristics are specified in the aforementioned stocktaking. Moreover, it specifies who the person in charge of the hardware is.

8.3 Staff Security

KAS BANK should make all efforts to verify that the staff complies with the minimal requirements to carry out its functions.

KAS BANK makes sure all employees comply with the security aspects in the employees handbook.

8.4 Physical and environmental security

KAS BANK makes all efforts to verify that the physical access to critical services and the physical risks of these elements are minimized. All procedures surrounding these security aspects are KAS BANK confidential, and therefore not written in this CPS.

8.5 System management security

KAS BANK makes security copies of its data and the data related to the provision of certification services periodically.

8.6 Business continuity plan

KAS BANK has a business continuity plan in order to protect the systems related to KAS BANK’s provision of certification services from faults or disasters.
8.7 Incidents

An incident is considered to be any anomaly that may affect the data security or the access to different computer platforms. KAS BANK has a procedure of notification and management of incidents. When these incidents take place, they are notified according to the established procedure and stored in a record of incidents which is monthly reviewed by a KAS BANK employee.

8.8 Compliance

All employees dealing with personal data have been correctly trained and informed about current legislation regulating data protection and about the measures to take when dealing with this type of information. KAS BANK has compliance procedures in place.
9 CERTIFICATES AND CERTIFICATES’ LISTS CHARACTERISTICS

9.1 Certificate’s characteristics

Depending on the certificate, it could be issued on a file or on cryptographic smartcard. The smartcard will be issued in the installations where KAS BANK’s CA is located as well as in the external installations, from a file created by KAS BANK for that purpose.

When the smartcards are engraved and stamped in external installations, security measures will be applied in order to prevent users’ private keys form being manipulated.

The validity period of the certificate is stipulated in it and should always comply with current legislation.

9.2 Certificates’ lists

KAS BANK’s revoked or suspended certificates will be published in a public repository by the authorized staff from the files generated by KAS BANK.

The Certificate Revocation List (CRL) will be available to all users at http://pki.kasbank.com/crl.asp/

Suspended and revoked certificates will be listed in the CRL during a period of three years. After this period, the entire certificate’s data will be removed from the CRL and will be deposited in the CA’s offices during a period of seven years.
10 OTHER

10.1 CPS and Certification Practices’ modification procedures

KAS BANK will be able to modify this CPS and the Certification Policy without affecting the quality of its certification services. The modifications should be justified from a legal, technical or commercial point of view.

10.2 Modification publication procedure

The modifications of the CPS and of the Certification Policy will be notified at the CA’s web page http://pki.kasbank.com.

10.3 Publication notification procedure

If the aforementioned modifications directly affect the subscriber and applicant’s rights and obligations, or the certificate's operating capacity on the part of users, subscribers and applicants will be notified.