

Obligation Policy Verpflichtungserklärung Politique d'obligation

Siemens CA

Version: 1.0
Date: 07.03.2024
Classification: Public / Unrestricted

Inhaltsverzeichnis / Table of Contents

- 1. English.....3
- 2. Deutsch4
- 3. Français.....5

Änderungshistorie / Release Notes

Version	Date	Author	Change Comment
1.0	March 07, 2024	CPKI Trust Center	First released version

1. English

Obligation of the applicant and the applicant's delegate

Siemens employees need a certificate from the Siemens Corporate PKI to carry out their work. In connection with the application for and use of such a certificate, you must observe a number of applicable regulations. The regulations that apply to you as an applicant or as an applicant's delegate are summarized in this document.

This Obligation Policy is consistent with the Siemens Certificate Policy (CP) and the Siemens Certificate Practice Statement (CPS). Both documents can be read or downloaded in PDF-Format at <https://www.Siemens.com/pki>.

1. I as an applicant or as an applicant's delegate affirm with my certificate application that:

- All the details used for a certificate application (given name, surname and e-mail address) are correct and complete.
Please note that Trusted data basis for digital certificates issued by Siemens CA is the Siemens Corporate Directory (SCD).
- I as an applicant will no longer use the signature function after the validity of the certificate expires or the certificate is revoked.
- I as an applicant will always keep my PIN secret for all my PKI token I have (Corporate ID card, Softtoken, VSC etc.) and I will not disclose my PKI token or leave it unattended.
- I as an applicant will immediately have my certificates revoked if one of my PKI token is lost or has been compromised. A certificate revocation can be processed on the PKI Self Service Portal under mypki.siemens.com (Revoke Certificate) or via e-mail to contact.pki@siemens.com.

2. When using the certificates, I as an applicant affirm that:

- All the information contained inside the certificate is true as far as I am aware or have knowledge of this information.
- I am responsible for protecting the PKI token and will protect my PIN against misuse, loss, disclosure and unauthorised use.
- Should an unauthorised party ever gain access to my token or my PIN, I will change this to a value that only I know without undue delay.
- Digital certificates and the private keys will be used exclusively for authorized purposes and in compliance with the [Siemens Certificate Policy \(CP\)](#), which also contain other technical and organisational information.

Review and Updates

This Obligation Policy but also referenced documents like [Siemens Certificate Policy \(CP\)](#) or [Siemens Certificate Practise Statement \(CPS\)](#) will be reviewed annually, or as necessary in case of changes to technology, regulations or organizational requirements.

2. Deutsch

Verpflichtung der Teilnehmer/innen und Bevollmächtigten

Zur Ausübung Ihrer Tätigkeit benötigen Sie ein Zertifikat aus der Siemens Corporate PKI. Im Zusammenhang mit der Beantragung und Nutzung eines solchen Zertifikats müssen Sie einige hierfür geltenden Regelungen beachten. Diese sind für Sie als Teilnehmer/in („applicant“) oder als Bevollmächtigte/r („delegate“) eines Teilnehmers/einer Teilnehmerin im Sinne der Siemens Certificate Policy geltenden Regelungen sind in diesem Dokument zusammengefasst.

Diese Verpflichtungserklärung (Obligation Policy) steht im Einklang mit der Siemens Certificate Policy (CP) und dem Siemens Certificate Practice Statement (CPS). Beide Dokumente können auf der Website der Siemens PKI <https://www.siemens.com/pki> direkt gelesen oder im PDF-Format heruntergeladen werden.

1. Bei Antragstellung versichere ich als Teilnehmer/in oder als Bevollmächtigte/r eines Teilnehmers/einer Teilnehmerin im oben erläuterten Sinne, dass:
 - alle Angaben im Zertifikatsantrag (Vorname, Nachname und E-Mail-Adresse) richtig und vollständig sind. Bitte beachten Sie, die vertrauensvolle Datenbasis für die Ausstellung digitaler Zertifikate von der Siemens CA ist das Siemens Corporate Directory (SCD).
 - ich als Teilnehmer/in die Signaturfunktion nach Ablauf der Gültigkeit des Zertifikats oder der Sperrung des Zertifikats nicht mehr nutzen werde.
 - ich als Teilnehmer/in die PIN für alle meine PKI Token (Firmenausweis, Softtoken, Virtual SmartCard etc.) stets geheim halte und meine PKI-Token nicht weitergeben oder unbeaufsichtigt lassen werde.
 - ich als Teilnehmer/in unverzüglich im Falle des Verlusts oder Missbrauchs des PKI-Tokens meine Zertifikate sperren lassen werde. Mögliche Sperrverfahren sind entweder eine Sperrung direkt im PKI Self-Service Portal unter mypki.siemens.com (Zertifikate revozieren) oder die Veranlassung der Sperrung per E-Mail an contact.pki@siemens.com.
2. Bei der Nutzung der Zertifikate versichere ich als Teilnehmer/in im oben erläuterten Sinne, ...
 - dass alle im Zertifikat enthaltenen Informationen der Wahrheit entsprechen, soweit ich von diesen Informationen Kenntnis oder Wissen habe.
 - dass ich für den Schutz des PKI-Token verantwortlich bin und ich meine PIN vor Missbrauch, Verlust, Preisgabe oder unbefugter Benutzung schütze.
 - dass ich, sollte dennoch ein Unbefugter jemals Zugang zu meinem Token oder meiner PIN erlangen, diese unverzüglich auf einen nur mir bekannten Wert ändere.
 - das Zertifikat bzw. den privaten Schlüssel ausschließlich für zugelassene Zwecke im Einklang mit den [Siemens Certificate Policy \(CP\)](#) zu verwenden, in denen auch weitere technische und organisatorische Informationen zu finden sind.

Überprüfung und Aktualisierung

Diese Verpflichtungserklärung sowie auch die referenzierten Dokumente, wie [Siemens Certificate Policy \(CP\)](#) oder [Siemens Certificate Practice Statement \(CPS\)](#) werden jährlich überprüft sowie zusätzlich bei Bedarf im Falle von Änderungen bzgl. Technologie, Vorschriften oder organisationsbezogenen Anforderungen aktualisiert.

3. Français

Obligation du participant ainsi que son délégué

Les employés de Siemens ont besoin d'un certificat de la part de la PKI Siemens (Siemens Corporate PKI) afin d'accomplir leur travail. En ce qui concerne la demande et l'utilisation d'un tel certificat, vous devez tenir compte de certaines règles applicables en la matière. Celles-ci sont résumées dans ce document pour vous en tant que participant (« applicant ») ou en tant que délégué (« delegate ») d'un participant, conformément aux règles applicables de la Siemens Certificate Policy.

Cette politique d'Obligation (Obligation Policy) est conforme à la politique de certificats de Siemens (Siemens Certificate Policy (CP)) ainsi qu'à la Déclaration de pratiques de certification (Siemens Certificate Practice Statement (CPS)). Ces deux documents sont disponibles en format PDF à l'adresse suivante <https://www.Siemens.com/pki>.

1. Lors de la demande, en tant que participant ou en tant que délégué d'un participant dans le sens expliqué ci-dessus, je confirme que:

- Tous les détails inclus dans la demande de certificat (Prénom, nom et adresse mail) sont corrects et complets.
Veuillez noter que la base de confiance pour les certificats digitaux émis par l'autorité de certification de Siemens (Siemens CA) est le répertoire Siemens Corporate Directory (SCD).
- En tant que participant, je n'utiliserais plus la fonctionnalité "signature digitale" après l'expiration ou la révocation de mon certificat.
- En tant que participant, je protégerais toujours mon code PIN pour tous les tokens PKI liés à mon compte (Corporate ID card, Softtoken, VSC etc.) et de protéger mes tokens et ne pas les laisser sans surveillance.
- En tant que participant, je révoquerais mes certificats si l'un de mes tokens PKI est perdu ou compromis. La révocation du certificat peut être faite de façon autonome sur le portail PKI sous mypki.siemens.com (Révoquer un Certificat) ou par e-mail à contact.pki@siemens.com.

2. En utilisant les certificats, en tant que participant je confirme que:

- Toutes les informations contenues dans le certificat sont correctes à ma connaissance, dans la mesure du possible.
- Je suis responsable de protéger mon token PKI ainsi que mon PIN contre la perte, divulgation ou toute utilisation abusive.
- Dans le cas où une personne non autorisée aurait eu accès à mon code PIN, je changerais ce dernier pour une valeur connue uniquement par moi-même le plus rapidement possible.
- Les certificats digitaux ainsi que les clés privées seront utilisés exclusivement pour des usages autorisés et en conformité avec [Siemens Certificate Policy \(CP\)](#), contenant des informations techniques et organisationnelles.

Révision et mises à jour

Cette politique d'obligation ainsi que les documents de référence comme [Siemens Certificate Policy \(CP\)](#) ou [Siemens Certificate Practise Statement \(CPS\)](#) seront révisés tous les ans, ou en cas de besoin dans le cas d'évolution de la technologie, les régulation ou des besoins organisationnels.