



Declaration of commitment / Verpflichtungserklärung /
Föreskrifter för användning av PKI / Verbintenisvesrklaring /
Déclaration d'engagement / Závazné vyhlásenie /
Závazné prohlášení / Kötelezettségvállalás

1. English	3
2. Deutsch.....	4
3. Swedish	5
4. Dutch	6
5. French.....	7
6. Czech	8
7. Hungarian	9

1. English

Declaration of commitment

As a requirement for the issue of certificates from UNIPER PKI, you must acknowledge the following duties and confirm your acknowledgement in your application.

The Certificate Policy (CP) and these Subscribers' Obligations are available for download in PDF-Format at <https://www.uniper.energy/pki>.

1. I affirm with my application that

- all the information in the application for the certificate (given name, family name and e-mail address) is correct and complete,
- I will no longer use the signature function after the validity of the certificate expires or the certificate is revoked,
- I will keep the PIN secret and I will not disclose my PKI token or leave it unattended, and • I will revoke my certificates if the PKI token is lost or has been compromised.

Possible blocking procedures that can also be implemented on behalf of colleagues:

PKI Portal:	https://pki.uniper.energy/ussp2
E-mail address:	Uniper DE GSD@dx.com

The PKI Portal function "Revoke Certificates / Delete Token" can be used by colleagues or service desk staff to revoke all certificates of a given KID. After one hour the user may request new certificates for a new PKI token, in case the KID's (IT account's) status is still active.

2. When using the certificates, I affirm that

- all the information contained in the certificate is true as far as I am aware or have knowledge of this information,
- I (and not D-TRUST as the UNIPER trust centre) am solely responsible for protecting the PKI token and will protect my PIN against misuse, loss, disclosure and unauthorised use,
- no unauthorised party has ever had access to my token or my PIN (and if they have had, I will change this immediately to a value that only I know before any damage can arise),
- the certificate and the private key will be used exclusively for permitted purposes in compliance with the [Uniper certificate policies](#), which also contain other technical and organisational information.

2. Deutsch

Verpflichtungserklärung

Voraussetzung für die Ausstellung von Zertifikaten aus der UNIPER PKI ist, dass Sie die folgenden Pflichten anerkennen und dies im Rahmen der Antragstellung bestätigen.

Die Certificate Policy (CP), und diese Verpflichtungserklärung (Subscribers' Obligations) können im PDF-Format von der Website der Uniper <https://www.uniper.energy/pki> herunter geladen werden.

1. Bei Antragstellung versichere ich, dass ...

- alle Angaben im Zertifikatsantrag (Vorname, Nachname und E-Mail-Adresse) richtig und vollständig sind,
- ich die Signaturfunktion nach Ablauf der Gültigkeit des Zertifikats oder der Sperrung des Zertifikats nicht mehr nutzen werde,
- ich die PIN stets geheim halten und meinen PKI-Token nicht weitergeben oder unbeaufsichtigt lassen werde und
- ich im Falle des Verlusts oder Missbrauchs des PKI-Tokens meine Zertifikate sperren werde.

Mögliche Sperrverfahren, die auch für Kollegen im Auftrag durchgeführt werden können:

PKI Portal:	https://pki.uniper.energy/ussp2
E-mail address:	Uniper_DE_GSD@dx.com

Die Sperrung über das PKI Portal mit der Funktion „Zertifikate sperren / Uniper Token löschen“ können durch Eingabe der KID durch einen Kollegen / den Servicedesk, dessen Zertifikate im Auftrag gesperrt werden. Nach einer Stunde können neue Zertifikate für ein neues PKI Token beantragt werden, sofern die KID nicht inaktiviert wurde.

2. Bei der Nutzung der Zertifikate versichere ich, ...

- dass alle im Zertifikat enthaltenen Informationen der Wahrheit entsprechen, soweit ich von diesen Informationen Kenntnis oder Wissen habe,
- dass ausschließlich ich für den Schutz des PKI-Token verantwortlich bin (und nicht die D-TRUST als UNIPER Trustcenter) und ich meine PIN vor Missbrauch, Verlust, Preisgabe oder unbefugter Benutzung schütze,
- dass kein Unbefugter jemals Zugang zu meinem Token oder meiner PIN hatte (wenn doch, ändere ich diese sofort auf einen nur mir bekannten Wert, bevor Schaden entstehen kann),
- das Zertifikat bzw. den privaten Schlüssel ausschließlich für zugelassene Zwecke im Einklang mit den [Zertifikatsrichtlinien der UNIPER](#) zu verwenden, in denen auch weitere technische und organisatorische Informationen zu finden sind.

3. Swedish

Föreskrifter för användning av PKI

En förutsättning för utfärdande av certifikat från UNIPER PKI är att Ni accepterar följande föreskrifter med denna ansökan. Uniper's Certifikatspolicy (CP) finns tillgängliga för nerladdning i PDF-format på <https://www.uniper.energy/pki>

1. Vid ansökan försäkrar jag, att...

- alla uppgifter i min ansökan om certifikat (förnamn, efternamn och e-postadress) är korrekta och fullständiga,
- jag inte längre kommer att använda signaturfunktionen efter utgången av certifikatets giltighetstid eller spärrandet av certifikatet,
- jag alltid kommer att hålla min PIN-kod hemlig och inte lämna mitt PKI-Token utan uppsikt och
- jag ifall att mitt PKI-Token försvinner eller utsätts för risk kommer att spärra mina certifikat.

Möjliga tillvägagångssätt för spärrning vilket även kan även göras av en kollega:

PKI Portal:	https://pki.uniper.energy/ussp2
E-post-adress:	Uniper_DE_GSD@dx.com

I PKI-portalen finns funktionen "Revoke Certificates / Delete Token" vilken kan användas av en kollega eller Global Service Desk för att återställa alla certifikat på ett KID. Efter en timma så kan användaren begära nya certifikat för ett nytt PKI-token om KID'et fortfarande är aktivt.

2. Vid nyttjande av certifikaten försäkrar jag, ...

- att all information som certifikatet innehåller är sanningsenliga, så långt jag har kännedom eller vetskap om innehållet,
- att jag uteslutande är ansvarig för att skydda mitt PKI-token (och inte D-TRUST som UNIPER Trustcenter) samt att jag skyddar min PIN-kod från otillåten användning,
- att ingen obehörig någonsin haft tillgång till mitt PKI-token eller min PIN-kod (om det skulle hända så ändrar jag dessa omedelbart innan någon skada kan uppstå), att använda certifikatet och den privata nyckeln endast används för tillåtna ändamål i överensstämmelse med Uniper's [Certifikatspolicy](#), vilka även innehåller teknisk och organisatorisk information.

4. Dutch

Verbintenisverklaring

Als voorwaarde voor de uitgifte van certificaten van Uniper van de PKI is gesteld dat de onderstaande verplichtingen door u worden geaccepteerd endat dit in uw aanvraagformulier expliciet wordt bevestigd. Het certificaat beleid en de bijbehorende gebruikers verplichtingen zijn beschikbaar in PDF formaat op <https://www.uniper.energy/pki>.

1. Voor de indiening van het verzoekgarandeer ik dat ...

- alle gegevens in het aanvraagformulier voor certificaten (voornaam, achternaam en e-mailadres) correct en volledig zijn
- ik de handtekening na het verstrijken van de geldigheid van het certificaat of de blokkade van het certificaat niet meer zal gebruiken,
- ik de pincode steeds geheim zal houden en mijn PKI-token niet zal afgeven of onbeheerd achter zal laten en
- ik in geval van verlies of bij misbruik van de PKI-token mijn certificaten zal blokkeren.

Mogelijke blokkades die ook voor collega's in opdracht uitgevoerd kunnen worden:

PKI Portal:	https://pki.uniper.energy/ussp2
e-mail-adres:	Uniper_DE_GSD@dx.com

De functie intrekken certificaten/verwijder token, beschikbaar op het PKI portaal, kan gebruikt worden door collega's of medewerkers van de Servicedesk om certificaten te verwijderen van een aangeven KID. Na 1 uur kan de gebruiker voor een nieuw PKI token nieuwe certificaten aanvragen mits de KID nog steeds actief is.

2. Bij het gebruik van de certificaten garandeer ik, ...

- dat alle gegevens in het certificaat waar zijn voor zover informatie aan mij bekend is gemaakt,
- dat alleen ik verantwoordelijk ben voor de bescherming van de PKI-token (en niet D-TRUST als UNIPER trustcenter) en ik mijn pincode tegen misbruik, verlies, openbaarmaking of ongeautoriseerd gebruik zal beveiligen,
- dat geen onbevoegde ooit toegang heeft gehad tot mijn token of mijn pincode (mocht dit toch het geval zijn, verander ik deze direct ineen waarde die alleen mij bekend is voordat er schade kan optreden).
- het certificaat resp. de privé sleutel uitsluitend voor toegestane doeleinden en in overeenstemming met de [certificaatrichtlijnen van Uniper](#) te gebruiken, waarin ook andere technische en organisatorische informatie te vinden is.

5. French

Déclaration d'engagement

La délivrance de certificats à partir de l'Infrastructure à Clés Publiques (ICP ou PKI en anglais) de UNIPER est possible sous réserve que vous acceptiez les obligations suivantes et que vous le confirmiez lorsque vous soumettez votre demande.

La politique de Sécurité (CP) est disponible en téléchargement au format PDF à l'adresse suivante : <https://www.uniper.energy/pki>.

1. Lors de la soumission de ma demande, j'atteste ...

- que toutes les informations fournies dans la demande de certificat (prénom, nom et adresse e-mail) sont exactes et complètes,
- que je n'utiliserai plus la fonction signature après l'expiration de la validité du certificat ou après son blocage,
- que je garderai le code PIN toujours secret, ne transmettrai à quiconque ma clé ICP ni ne la laisserai sans surveillance et
- que je bloquerai mes certificats si la clé est perdue ou compromise.

Procédures de blocage possible qui peuvent être aussi exécutées pour des collègues qui le demande

PKI Portal:	https://pki.uniper.energy/ussp2
Adresse E-Mail:	Uniper DE GSD@dx.com

La fonction "Révoquer les certificats / Supprimer Token" peut être utilisé par des collègues ou du personnel de service desk depuis le portail PKI, une heure après, l'utilisateur peut demander de nouveaux certificats.

2. Lors de l'utilisation des certificats, j'atteste ...

- que toutes les informations contenues dans le certificat sont sincères pour autant que j'ai connaissance de celles-ci,
- que moi seul(e) suis responsable de la protection de la clé ICP (et non pas la D-TRUST en sa qualité de Trustcenter de UNIPER) et que je protège mon code PIN de tout abus, perte, abandon ou utilisation illicite,
- qu'aucune personne non autorisée n'avait accès à ma clé ou mon code de PIN (dans le cas contraire, je le change immédiatement pour un code connu uniquement par moi-même avant la survenance d'un quelconque dommage,
- utiliser le certificat ou la clé privée exclusivement aux fins admises en conformité avec les [directives portant sur les certificats d'Uniper](#), qui contiennent de plus amples informations de nature technique et organisationnelle.

6. Czech

Závazné prohlášení

Předpokladem pro vystavení certifikátů ze strany UNIPER PKI je vaše uznání následujících povinností a jejich potvrzení v rámci podání žádosti.

Certifikační politika (CP) a povinnosti odběratelů certifikačních služeb jsou dostupné ke stažení in PDF formátu na tomto odkaze <https://www.uniper.energy/pki>.

1. Při podání žádosti prohlašuji, že ...

- všechny údaje v žádosti o certifikát (jméno, příjmení a e-mailová adresa) jsou správné a úplné;
- po uplynutí platnosti certifikátu nebo jeho zablokování už nebudu využívat funkci podpisu;
- budu vždy držet v tajnosti svůj PIN, nikomu nepředám svůj token PKI, neponechám jej nikde bez dozoru; a
- v případě ztráty nebo kompromitace PKI tokenu své certifikáty zneplatním (odvolám).

Kontakty pro možné blokace, které lze v zastoupení provést i za kolegy:

Portál PKI:	https://pki.uniper.energy/ussp2
E-mailová adresa:	Uniper DE_GSD@dx.com

Volba na PKI portálu “Odvolat certifikáty/Smazat token” může být aktivována kolegy nebo zaměstnancem Service Desku k odvolání platnosti všech certifikátů pro požadovaný KID. Po jedné hodině může dotčený uživatel požadovat vystavení nového certifikátu na nový PKI token v případě, že status KIDu (IT účtu) tohoto uživatele je stále aktivní.

2. Při využívání certifikátů potvrzuji, že ...

- všechny informace uvedené v certifikátu odpovídají skutečnosti, pokud jsou mi tyto informace známy;
- za ochranu PKI tokenu odpovídám pouze já (a nikoliv D-TRUST jako centrum zabezpečení společnosti UNIPER Trustcenter) a budu svůj PIN chránit před zneužitím, ztrátou, vyrazením nebo neoprávněným použitím;
- k mému tokenu nebude mít přístup žádná neoprávněná osoba a nikdo takový nebude mít k dispozici ani můj PIN (a pokud se tak stane, ihned jej změním na hodnotu známou pouze mně, ještě než budou moci vzniknout nějaké škody);

certifikát, resp. soukromý klíč, budu používat výhradně k přípustným účelům v souladu se směrnicemi [společnosti Uniper ohledně certifikátů](#), které zahrnují i další technické a organizační informace.

7. Hungarian

Kötelezettségvállalás

Az Uniper PKI-ből akkor lehet kiállítani a tanúsítványokat, ha Ön elfogadja a következő feltételeket, és ezt kérelem formájában megerősíti.

A Hitelesítési Rend (Certificate Policy, CP) és az aláírói kötelezettségek (Subscribers' Obligations) letölthetőek PDF formátumban a <https://www.uniper.energy/pki> oldalról.

1. A kérelemmel kapcsolatban vállalom, hogy...

- a tanúsítványkérelemben szereplő valamennyi adat (utónév, családnév és e-mail cím) helyes és hiánytalan,
- a tanúsítvány érvényességének lejártá vagy a tanúsítvány visszavonása után nem használom tovább az aláírás funkciót,
- a PIN kódot mindig titokban tartom, és a PKI kulcsomat nem adom tovább, illetve nem hagyom felügyelet nélkül, valamint
- a PKI kulcs elvesztése vagy a PKI kulccsal való visszaélés esetén visszavonom a tanúsítványaimat.

A munkatársak megbízásából is lebonyolítható tanúsítvány visszavonási eljárások:

PKI portál:	https://pki.uniper.energy/ussp2
e-mail cím:	Uniper_DE_GSD@dx.com

A dolgozók és a Service Desk munkatársai használhatják PKI portálon található "Tanúsítvány Visszavonása / Token Törlése" funkciókat az adott KID-hez tartozó összes tanúsítvány visszavonására. Ha a KID továbbra is aktív, a felhasználó egy óra elteltével kérhet új tanúsítványokat az új PKI tokenhez.

2. A tanúsítványok használata során vállalom, hogy ...

- a tanúsítványban szereplő valamennyi információ legjobb tudomásom szerint megfelel a valóságnak,
- kizárólag én felelek a PKI kulcs védelméért (nem pedig a D-TRUST, az UNIPER Adatvédelmi központja), és gondoskodom róla, hogy ne élhessenek vissza a PIN kódommal, ne vesszen el, ne kerüljön nyilvánosságra, illetve, hogy illetéktelen személyek ne használhassák,
- illetéktelen személyek soha ne férhessenek hozzá a kulcsomhoz vagy a PIN kódomhoz (ha mégis, haladéktalanul megváltoztatom azt egy kizárólag általam ismert értékre, mielőtt kár keletkezne),
- a tanúsítványt és a személyes kulcsot **kizárólag az Uniper tanúsítványokra** vonatkozó irányelveivel összhangban lévő engedélyezett célokra használom, amelyek további műszaki és szervezési információkat is tartalmaznak.