



TRANSLATION

APPROVED BY
Management Board Resolution
of Siemens LLC
dd. 02 July 2018

Siemens Electronic Document Management System Policy

**Moscow
2018**

Index

Terms and abbreviations	4
1. General	9
1.1 Details of Siemens EDM system owner.....	9
1.2 Operating principles.....	9
2. Use of Siemens digital signature in Siemens System	12
2.1 Exchange of electronic documents	12
2.2 Recording documents dispatch and receipt time	12
2.3 Restrictions.....	12
2.4 Legal force of documents signed with Siemens digital signature	12
2.5 Use of CIPF	13
2.6 Personal data and confidentiality.....	13
2.7 Replacement of keys	13
2.8 Types of certificates issued by CA of Siemens AG	13
2.9 Types of CIPF.....	14
3. Rights and obligations of parties.....	14
3.1 Obligations of EDF Operator	14
3.2 Rights of the Operator	14
3.3 Obligations of EDF participant	15
3.4 Rights of EDF participant.....	15
3.5 Withdrawal of EDF participant from EDF	15
4. Liability of parties	16
5. Revocation of consent to personal data processing	18
6. Confidentiality	18
7. Force majeure	19
8. Procedures for use of CIPF.....	19
8.1 Types of key media for Siemens DS	19
8.2 Ordering key media for Siemens DS.....	19
8.3 Generation of keys for Siemens DS.....	20
8.4 Creation of request for certificate	20
8.5 Activation of key media for Siemens DS.....	20
8.6 Transportation of smart card	20
8.7 Operation of key media for Siemens DS.....	21
8.8 Replacement of keys	21
8.9 Decommissioning of key media for Siemens DS	21
Unrestricted	2

SIEMENS

8.10 Requirements for EDF workplaces	22
9. Siemens digital signature	22
9.1 Generation of Siemens digital signature	22
9.2 Procedure for Siemens digital signature verification	22
10. Settlement of disputes.....	23
11. Key compromise response.....	23
12. Hierarchy of regulatory documents	24
13. Governing law and jurisdiction.....	24
Appendix 1 - Application for Accession to EDF Policy Siemens LLC (form for legal entities)	25
Appendix 2 - Application for Accession to EDF Policy Siemens LLC (form for individuals)	27
Appendix 3 - Application for Accession to EDF Policy Siemens LLC (form for Siemens employees)	29
Appendix 4 - Form of request for issue of smart card (form for legal persons)	31
Appendix 5 - Form of request for issue of smart card (form for individuals)	32
Appendix 6 - Rules for handling smart cards for EDF participants except for Siemens employees.....	33
Appendix 7 - Provision on the use of unqualified enhanced Siemens digital signature as a part of legally relevant electronic document flow in Siemens LLC	38
Appendix 8 - Rules for handling physical and virtual smart cards (for Siemens employees only)	43
Appendix 9 – License of EDF Operator issued to Siemens LLC by the FSS.....	51

This Policy is updated as needed. Each new revision is duly approved before issue.

This document is published on the website: <http://siemens.ru/digital-id>.

Terms and abbreviations

Electronic Document Authorship – attribution of an electronic document to either Party. Electronic Document Authorship, so far as this Policy concerns, is determined by verifying authenticity of Siemens DS using CIPF.

Security Administrator– an officer of the EDF Organizer responsible for CIPF operation and cryptographic keys management.

EDF Administrator – an officer of the EDF Organizer responsible for EDF maintenance and EDF software operation.

Commissioning (Decommissioning) of Siemens Digital Signature Public Verification Key Certificate in EDF – the procedure for recording (deleting) details of a public verification key certificate for Siemens digital signature and the authorities of its owner in EDF software. The date as from which a public verification key certificate for Siemens digital signature is considered commissioned (decommissioned), assumed corresponding to the date of commissioning (decommissioning) of a respective Siemens public verification key certificate as part of the EDF.

Virtual Smart Card – a virtual medium for cryptographic keys, programmable analogue of a physical smart card.

Owner of Public Verification Key Certificate – a person issued a public verification key certificate for Siemens digital signature in the manner described in this Policy. As part of the Siemens EDF, owners of public verification key certificates shall be EDF participants.

Business Partner – a legal or natural person (other than an employee of one of the Siemens Group companies) having acceded to this Policy and participating in the electronic document flow.

Application for Accession to EDF Policy – an agreement made between Siemens LLC and a legal or natural person participating in the electronic document flow for the accession of such legal or natural person to this Policy.

SIEMENS

IS – an authorized officer of the Siemens Information Security Function.

Siemens Public Verification Key – a unique sequence of symbols unambiguously associated with a Siemens private key and designed for verifying authenticity of Siemens digital signature.

Siemens Private Key – a unique sequence of symbols designed for generating Siemens digital signature.

Conflict Situation – a situation necessitating the settlement of issues of recognizing or refusing to recognize the authorship and (or) integrity of electronic documents signed with Siemens DS.

Correct Electronic Document – an electronic document which has passed the procedure of verifying authenticity of Siemens DS, file name, file format and document form and was found correct (conforming to the terms and conditions hereof).

Cryptographic Key (Key) – a generic name for Siemens private key and Siemens digital signature public verification key.

Incorrect Electronic Document – an electronic document which has failed the procedure of verifying authenticity Siemens DS, and (or) file name, and (or) file format, and (or) document form.

Electronic Document Processing – generation, storage, reorganization and visualization of an electronic document.

Siemens EDF Operator, System Operator, EDF Operator – a legal entity owning the Siemens EDF, software and hardware necessary for its operation and providing EDF Participants with an opportunity to participate in electronic document flow, and performing other functions in accordance herewith. The Siemens EDF Operator is Siemens LLC.

OS – an operating system.

EDF Risk (risk) – probability of damage sustained by the EDF Organizer and (or) an EDF Participant as a result of unauthorized impact to the EDF.

Certificate – an electronic document or paper document issued by a certification authority or a designee of a certification authority and confirming the attribution of a Siemens public verification key to an owner of a Siemens public verification key certificate.

Electronic Document Management System (hereinafter the “Siemens Electronic Document Management System”, “Siemens System” “EDF”, “EDM System”) – an
Unrestricted

SIEMENS

organizational and technical electronic document management system of the Siemens System Operator being a combination of regulatory references, software, information and hardware, computer facilities and databases designed for transfer of electronic documents, electronic copies of documents, in particular, those ciphered and signed with Siemens DS.

CIPF – a cryptographic information protection facility.

Smart Card – a physical medium for Siemens private keys.

Information Protection Facilities – software and hardware facilities preventing unauthorized access and/or unauthorized modification of information system data.

Certification authority's Facilities – software and (or) hardware facilities used to implement the functions of a certification authority.

Siemens Encryption Facilities – encryption (cryptographic) facilities used to implement at least one of the following functions: generation of Siemens digital signature, verification of Siemens digital signature, generation of a Siemens private key and Siemens digital signature public verification key.

EDF Participant (Business Partner, employee of Siemens LLC) – an individual, legal entity (or authorized employee of a legal entity), employee of Siemens LLC who acceded to this Policy and participates in the electronic document flow.

Authorized EDF Officer – an officer of Siemens LLC authorized by the Siemens management to accept EDF accession requests, issue public verification key certificates on behalf of the CA of Siemens AG, accept requests from EDF participants for revocation of certificates or revocation of consents to personal data processing. An authorized EDF officer interacts with all EDF participants except for employees of Siemens LLC. Email address of an authorized EDF officer: digitalsignature.ru@siemens.com

CA – a certification authority authorized to issue public key certificates for use in the Siemens EDF, a legal entity performing the functions of generating and issuing public key certificates for Siemens digital signatures and other functions. In the Siemens EDF, an entity authorized by a certification authority is the CA of Siemens AG (Germany, Munich). CA documents are accessible in the Internet on the website <https://www.siemens.com/pki/>

Contact details of the Certification authority of Siemens AG (Germany):

Siemens AG

GS IT ISEC

SIEMENS

Responsible officer of CA

Munich 81739, Federal Republic of Germany

E-mail: contact.pki@siemens.com

The CA of Siemens AG (Germany) carries out its activities, in particular, issues public key certificates, in accordance with the laws of the Federal Republic of Germany and the international standards. Public key certificates for Siemens digital signature issued by the CA of Siemens AG are generated in accordance with the laws of the Federal Republic of Germany and the international standards. In the Russian Federation, this Siemens digital signature fully conforms to all properties of an enhanced encrypted unqualified signature described in Federal Law On Digital Signature No. FZ-63 dd. April 6, 2011 and is recognized an enhanced unqualified signature. An enhanced Siemens digital signature generated with the use of certificates issued by the CA of Siemens AG and electronic documents or electronic messages signed with it have a full legal force and effect in the Russian Federation.

The trusted partner of the Certification authority of Siemens AG (Germany) in the Russian Federation is Siemens LLC, being the EDF Operator.

Electronic Document Integrity – a property of an electronic document consisting in its existence in undistorted form (invariable as regards its certain fixed state).

Registration Authority – a hardware-software complex designed for registering owners of certificates, being a CA component.

Certification Center (CC, LRA) – a hardware-software complex designed for receiving requests for certification and issuing certificates, being a CA component.

Siemens Digital Signature (Siemens DS) – a digital used in the Siemens EDF and generated in accordance with the laws of the Federal Republic of Germany and the international standards using public key certificates issued exclusively by the CA of Siemens AG. Siemens DS is information configured in electronic form which is connected to other information in electronic form (signed information) or otherwise related to such information and which is used to identify a person signing the information (detail of an electronic document designed to protect an electronic document against forgery and used to identify a public key certificate owner, and to confirm the absence of information distortions in an electronic document). As used in this Policy, this term denotes a unqualified enhanced signature according to Federal Law of Russia On Digital Signature No. FZ-63 dd. 06.04.2011.

SIEMENS

Web-Based Electronic Mail (electronic mail) – an electronic mail system using open Internet channels and designed for transfer, receipt and temporary storage of electronic mail messages, including those containing electronic documents of the parties. The parties are responsible for using access to, and maintaining operability of, a web-based electronic mail on the terms and conditions established as part of the contractual relationships of each party with a provider of respective web-based telecommunication services.

Electronic Message (EM) – a message in which information relevant to the parties is presented in digital form and appropriate format. An electronic message can be configured as a document using software specified in this Policy.

Electronic Mail Message (EMM, electronic message) – an electronic message arranged in a format assumed for electronic mail and designed for electronic mail transfer via Internet. An electronic mail message may contain electronic mail enclosures.

Electronic Mail Enclosure (EME, electronic enclosure) – a file with an electronic document which is attached as an electronic mail message.

Electronic Document – a document in which information is presented in digital form and appropriate format. An electronic document, as provided for in this Policy, shall be signed with Siemens DS. An electronic document completed in accordance with this Policy has full legal force for EDF participants. The list of document types, for which legal relevance is ensured as part of the Siemens EDF system, is to be separately determined and approved.

Electronic Document Flow (EDF) – exchange of electronic documents in accordance with this Policy.

1. General

This document is a user manual intended for participants of the Siemens Electronic Document Management System (EDMS). It contains the information describing the operating principles of the Siemens system and its functional capabilities.

1.1 Details of Siemens EDM system owner

The owner and organizer of the Siemens Electronic Document Management System in the Russian Federation is Siemens Limited Liability Company (abbreviated: Siemens LLC).

Place of business: Bolshaya Tatarskaya Str. 9, Moscow 115184.

The Siemens EDF owner is engaged in the operation and maintenance of the Siemens EDF. The address of the web-based system owner is:

<http://www.siemens.ru/>.

The Electronic Document Management System of Siemens consists of a number of functional subsystems:

The subsystem for transfer and storage of electronic documents consists of:

- a) SAP GP1;
- b) ReadSoft;
- c) LiveLink;
- d) DSC (Document Service Center) system;
- e) Siemens mail system, including client software Microsoft Outlook;
- f) File on network drives.

The subsystem for ensuring legal relevance of electronic documents consists of:

- a) Smart cards;
- b) Information protection facilities;
- c) Facilities of Certification authority of Siemens AG (Germany, Munich).

1.2 Operating principles

This Policy sets out the procedures for implementing the following processes:

- a) Legally relevant work with electronic documents.
- b) Procedures for operation of a cryptographic key, digital certificate for the Siemens digital signature.
- c) Forwarding, processing, reviewing necessary documents (electronic copies of documents).

SIEMENS

d) Other processes discussed in this Policy and other documents referred to in section 12 hereof.

All other documents of the Siemens System Operator are based on this Policy and, as such, are non-contradictory.

This Policy includes the main functional requirements for the Siemens system set out herein or in the agreements made with the participants.

This Policy is an offer which the EDF participants accept by signing the Application for EDF Accession to this Policy. Depending on the status of an EDF participant, the Application for Accession to EDF Policy is signed as per the form of Appendix 1 – for legal entities, as per the form of Appendix 2 – for individuals and as per the form of Appendix 3 – the employees of Siemens LLC.

The acceptance implies consent with all provisions of this Policy and the duties of complying therewith. As from the acceptance, an EDF participant is deemed to have acceded to this Policy and become a party thereto.

By acceding to this Policy, an EDF participant represents that it has fully familiarized itself with this Policy, and the Policy does not contain terms or conditions clearly onerous for an EDF participant.

The accession of a Party to the Policy means complete acceptance of the terms and conditions of this Policy and all its appendices and related documents in the revision effective as of the accession date.

The relation of other documents to this Policy is described in section 12.

The Party acceding this Policy consents to all future amendments (modifications) made hereto in accordance with the terms and conditions of this Policy.

Neither termination, nor revision of this Policy relieved the Parties of their obligations arising before the said date of termination or revision hereof, as well as their liability for failure to perform (improper performance of) the same.

The putting into effect, amending (modifying) of this Policy, including appendices hereto shall be the responsibility of the Siemens System Operator – Siemens LLC.

EDF participants shall be notified of the putting into effect, amending (modifying) of this Policy by the Siemens System Operator by way of mandatory posting of this Policy or amendments (modifications) hereto in the Internet on the website:

All amendments (modifications) made by the Siemens System Operator in the Policy, provided they are unrelated to changes in the applicable legislation, shall become binding within thirty (30) days of posting such amendments and modifications hereto on the website of the Siemens System Operator.

All amendments (modifications) made by the Siemens System Operator in the Policy to changes in the applicable legislation shall become effective simultaneously with the coming into effect of such changes (additions) in regulatory instruments, unless otherwise stated in a respective amendment (modification).

Any amendments and modifications in the Policy, as from their coming into effect, shall apply to all persons acceding to this Policy, including those who acceded hereto before the effective date of respective amendments (modifications).

All appendices, amendments and modifications to this Policy shall make an integral and an inseparable part hereof.

An EDF participant shall be deemed to have acknowledged the binding force of a new revision of this Policy if the Siemens System Operator does not receive a notice of an EDF participant of non-acceptance of a new revision hereof before the effective date of such new revision.

The notice of non-acceptance of a new revision of this Policy shall be sent by an EDF participant to an EDF officer in free form. If an EDF participant fails to give a notice of non-acceptance to an EDF officer within fifteen (15) days of the new version publication date, an EDF participant shall be deemed to have accepted a new version of the published EDF Policy.

The receipt of the above notice by the Siemens System Operator entails the revocation of a public key certificate held by an EDF participant and the return of a smart card (blocking of a virtual smart card). Any transactions and actions (operation) which remained unfinished at the time of access termination for an EDF participant shall be covered by the previous revision of this Policy.

After being notified of non-acceptance of a new revision hereof an Authorized EDF Officer shall agree upon the smart card return procedure with an EDF participant. The following smart card return options are acceptable: personally in the office of Siemens LLC located at Bolshaya Tatarskaya St. 9, Moscow, or by courier at the same address.

SIEMENS

The Siemens System Operator shall ensure confidentiality of the details of EDF participants as regards all the interacting parties.

2. Use of Siemens digital signature in Siemens System

An electronic document signed with Siemens DS of an EDF participant shall have the same legal force as a paper document signed in person (and affixed with the seal where necessary) and entails legal consequences attributable to this document. The availability of Siemens digital signature assigned to an EDF participant means that authenticity and accuracy of such documents and details is confirmed by an EDF participant.

2.1 Exchange of electronic documents

The exchange of electronic documents signed with a unqualified enhanced Siemens digital signature available to an EDF participant is a legally relevant electronic document flow.

When using Siemens DS, EDF participants shall abide by the laws of Germany, provisions of this Policy, and other documents referred to in section 12 hereof.

2.2 Recording documents dispatch and receipt time

The time of generation, dispatch and receipt of all electronic documents in the Siemens system is recorded according to the time of the server on which the Siemens system software operates. The Siemens System Operator is responsible for information security of the server timing control system.

When completing documents and forms in the Siemens system, an EDF participant shall monitor the data entry in the following manner: each file being attached is subject to virus test and size and format check. In the Siemens system, an EDF participant may use files up to 10 Mb. The permissible file formats are: pdf, doc, docx, xls, xlsx.

2.3 Restrictions

The Siemens System Operator is entitled to reject incorrect electronic documents, which do not meet the requirements of clause 2.2 in the second paragraph hereof, without considering the documents and data contained therein, and to deny an EDF participant certain actions or services the performance of which would require the provision of such documents and details.

The Siemens System Operator is not entitled to reject correct electronic documents.

An EDF participant shall be responsible for conformity of the contents of an electronic copy with the contents of an original paper document where an electronic document is a digitalized copy of a paper document.

2.4 Legal force of documents signed with Siemens digital signature

SIEMENS

EDF Electronic documents bearing Siemens DS, as used in the information exchange of EDF participants, shall have the same legal force as paper documents signed by authorized representatives and affixed with imprints of seals of EDF participants (regardless of whether such documents are available in hard copy or not).

2.5 Use of CIPF

EDF participants acknowledge that their CIPFs bearing Siemens DS and encryption are sufficient to ensure confidentiality and authenticity of electronic documents of the parties and evidence that an electronic document:

- a) originates from an EDF participant (confirmation of document authorship);
- b) was not changed during its transfer in electronic form as part of the information exchange of EDF participants (confirmation of document integrity).

2.6 Personal data and confidentiality

Transfer of electronic documents (electronic copies of documents) by an EDF participant using Siemens EDF implies the consent of an EDF participant (its authorized representatives) to the use (processing) of their personal data contained in the paper documents and (or) electronic documents (electronic copies of documents) being transferred.

The information to be included in public verification key certificates for Siemens digital signature is not confidential. The owner of a public verification key certificate for Siemens digital signature is aware of, and consents to, the publication of its personal data in a public verification key certificate for Siemens digital signature.

2.7 Replacement of keys

Replacement of public keys for Siemens DS does not affect the legal force of an electronic document signed with Siemens DS using a public key valid as of the signing date in accordance with this Policy.

2.8 Types of certificates issued by CA of Siemens AG

In accordance with its internal Policy (Certification Policy of the Certification authority of Siemens AG, Germany), CA of Siemens AG may issue unqualified enhanced certificates for the following categories of EDF participants:

- a) Siemens employee – EDF participant as defined in this Policy.
- b) Business Partner – natural or legal person, EDF participant as defined in this Policy.

SIEMENS

The procedure for issuing certificates is established in accordance with the above mentioned Certificate Policy and other applicable documents and procedures of the CA of Siemens AG.

2.9 Types of CIPF

Smart cards, virtual smart cards and other key media distributed by the EDF Operator can be used as virtual media for public keys of Siemens DS.

The use of virtual smart cards is only permissible for Siemens employees. Virtual smart cards shall not leave the secure network of Siemens LLC.

3. Rights and obligations of parties

3.1 Obligations of EDF Operator

Comply with the current laws, provisions of this Policy, documents referred to in section 12 hereof, and the contracts or agreements made between EDF participants.

Ensure operability and normal functioning of the Siemens system in accordance with this Policy. The Siemens System Operator shall ensure reliable functioning of the software and hardware used for the performance the functions provided for in this Policy and agreements made with an EDF participant.

As from accreditation in the Siemens system, allow an EDF participant an opportunity to obtain a CIPF, smart card with keys, and a public key certificate for Siemens digital signature in accordance with this Policy, and the Agreements made between EDF participants. Accreditation in the Siemens system shall be recognized as from the approval of an EDF participant's request for EDF accession by the EDF Operator.

Ensure the use of electronic documents in the Siemens system in accordance with current laws and the provisions of this Policy.

Arrange for electronic document flow between EDF participants.

3.2 Rights of the Operator

Process, verification and use of documents (electronic copies of documents) and data sent as part of EDF, and use such document and data in any other way (subject to the confidentiality provisions).

Carry out scheduled maintenance and adjustments to the software and hardware complex of the Siemens system. A specific date and time of the performance maintenance works shall be determined by the System Operator without coordination with EDF participants.

SIEMENS

Take other actions as provided for in this Policy, other documents referred to in section 12 hereof, and the contracts or agreements made between EDF participants.

Use other rights assigned by the current laws and provided for in this Policy, and the contracts or agreements made between EDF participants.

3.3 Obligations of EDF participant

Comply with the current laws, this Policy, other documents referred to in section 12 hereof, and the terms and conditions of contracts and agreements made between EDF participants.

Ensure confidentiality of cryptographic keys for digital signatures and, in particular, prohibit the use of its public keys without its consent.

Notify the certification authority and IS having issued a digital certificate for Siemens digital signature about violation of confidentiality of cryptographic keys for Siemens digital signature within one working day of becoming aware of such violation.

To notify the certification authority of a violation, follow the card blocking procedure at the link: <https://pkiss-emergency.siemens.com/>.

To notify the IS, a letter in free form shall be sent at: digitalsignature.ru@siemens.com.

Refrain from using a public key for Siemens digital signature if there are grounds to suggest that confidentiality of the key is disturbed.

3.4 Rights of EDF participant

Send documents, electronic copies of documents, draft documents to the Siemens system.

Obtain documents, electronic copies of documents, draft documents from the Siemens system.

Use other rights assigned by the current laws and provided for in this Policy.

Take other actions as provided for in this Policy, other documents referred to in section 12 hereof, and the contracts or agreements made between EDF participants.

3.5 Withdrawal of EDF participant from EDF

If an EDF participant (except for Siemens employees) elects to withdraw from EDF, it shall send a notice of withdrawal to the Authorized EDF Officer in free form at least thirty (30) days before withdrawal.

If an EDF participant (except for Siemens employees) acceded to this Policy under a term agreement, the withdrawal of this participant from EDF is recognized upon fulfillment of the

SIEMENS

term agreement. After termination of the term agreement, an EDF participant send a notice of withdrawal to the Authorized EDF Officer in free form at least ten (10) days before withdrawal.

The Authorized EDF Officer shall within one day of receiving a notice of withdrawal from an EDF participant revoke the certificates held by an EDF participant.

An EDF participant (Siemens employee) withdraws from EDF at the time of termination of his/her employment.

4. Liability of parties

The Siemens EDF Operator shall not be liable for damage of any kind and other losses incurred by an EDF participant as a result of failure to observe the provisions of this Policy, and the terms and conditions of the contracts and agreements made between EDF participants, as well as in the following events:

a) An EDF participant does not have computer hardware with the necessary set of hardware and software capabilities meeting the legal relevance requirements for Siemens EDF.

b) The available computer hardware has certain hardware and software limitations and settings preventing an EDF participant from normally sending electronic messages to the Siemens EDF.

c) Electronic messages cannot be sent to the Siemens EDF because of a virus in the computer hardware.

d) Certain failures occur in the operation of network systems, as well as limitations and faults of the hardware-software complex, which necessitate unforeseen emergency temporary shutoffs from the Internet and hinder the normal exchange with the Siemens EDF.

e) A digital certificate for a public key certificate for Siemens digital signature or an EDF participant's certificate is suspended.

f) An EDF participant, its employees, or designees disclose the identification data (PIN code, login, password) necessary for using the keys in the Siemens EDF.

The Siemens EDF Operator shall not be liable for damage of any kind and other losses incurred by an EDF participant due to insufficient familiarization with the information concerning the Siemens EDF operation and relationships between EDF participants, including:

a) Lack of knowledge of the current laws, this Policy and other documents referred to in section 12 hereof by an EDF participant.

SIEMENS

b) Ignorance, failure to perform, or improper performance of all requirements and procedures established by the current laws or provided for in this Policy, in particular, where such ignorance, failure to perform, or improper performance resulting in the incurrence by an EDF participant of additional, excessive, overly or unplanned liabilities to the Siemens EDF Operator or other EDF participants, and/or adversely affected the commercial activities and business reputation of an EDF participant as part of the Siemens EDF;

c) Failure to observe the rules for storage of public keys for Siemens digital signature or digital certificates, or their transfer (in particular, by an employee of an EDF participant) to any unauthorized third parties;

d) Actions taken by third parties in the Siemens EDF and/or with the Siemens DS (in particular, due to a lack of competence and knowledge of the current laws and the provisions of this Policy), which has resulted in the incurrence by an EDF participant of additional, excessive, overly or unplanned liabilities to Siemens, other EDF participants, or other third parties.

e) Failure to perform, or improper performance of requirements established by the current laws, this Policy, and the contracts or agreements made between EDF participants.

The Siemens System Operator shall not be liable for the quality of lines and operation of communication facilities, failures of telephone or other communication, failures of server equipment used to physically deploy the Siemens system.

The Siemens System Operator shall not be liable to an EDF participant for delays and interruptions of the document flow not immediately attributable to the System Operator or its actions, as well as for damage caused as a result of any circumstances beyond the reasonable control of the System Operator (fire, flood or other acts of God, war, riot, strike, equipment failure, computer virus impact, failures of power supply and telecommunication networks or other utilities, as well as other such events). The Siemens System Operator shall not be liable for operability of cryptographic keys for Siemens digital signature or digital certificates for Siemens digital signature held by EDF participants.

The rights and obligations under transactions carried out by an EDF participant, in particular, using a hardware-software complex to ensure legal relevance of the Siemens EDF, shall arise immediately with EDF participants between which a contract and/or agreement is made.

If the implementation of EDF becomes impossible (for any reason), EDF participants shall immediately inform each other of same stating the reason and the expected period for

SIEMENS

restoring the EDF. In this case, so far as such impossibility persists, the exchange of documents and electronic messages shall be arranged on paper.

5. Revocation of consent to personal data processing

An EDF participant shall have the right to revoke its consent to personal data processing. For this, it shall notify the Authorized EDF Officer by giving a written notice in free form at least thirty (30) days before revoking its consent.

A notice can be sent to the Authorized EDF Officer by electronic mail, post (courier or registered letter return receipt requested). A notice becomes binding for the System Operator upon its actual receipt.

If a personal data owner revokes its consent to personal data processing, the System Operator shall stop their processing and, where such personal data is no longer needed for personal data processing, shall destroy the same within thirty (30) days of receiving a revocation notice.

The receipt of a revocation notice by the Siemens System Operator entails the revocation of a public key certificate held by an EDF participant.

6. Confidentiality

The EDF participants are not entitled to disclose any confidential and/or proprietary information of either party contained in the contracts and agreements made between EDF participants.

Confidential information shall be deemed any information or details, regardless of the form of presentation or medium, meeting the following criteria:

- a) The owning of this information may ensure economic benefits or advantages as against persons who do not own it;
- b) This information is not publicly known or legally accessible through other sources;
- c) This information was not previously disclosed by the owner to third parties without the confidentiality obligation;
- d) This information was in possession of the Siemens System Operator under the confidentiality obligation;
- e) The owner of this information takes actions to ensure its confidentiality.

SIEMENS

The Siemens System Operator undertakes not to disclose the following confidential information:

- a) Data obtained as part of EDF;
- b) Personal data of an EDF participant;
- c) Details of the contracts and agreements made between EDF participants by using the Siemens system.

If the confidential information has to be disclosed to public authorities or agencies, an EDF participant who disclosed such information shall restrict the disclosure by the minimum required scope and immediately notify the EDF participants concerned of the subject matter of such disclosure to a maximum extent possible under the circumstances.

7. Force majeure

The parties shall be relieved of their liability for failure to perform or incomplete performance of the obligations undertaken under this Policy where such failure was caused by force majeure, namely: acts of God, epidemics, explosions, fires, acts of government and other emergency events. In this case, the period of performance of the parties' obligations hereunder shall be extended proportionally to the time during which such circumstances persisted.

The party affected by force majeure shall immediately give a written notice to the Siemens System Operator and the EDF participant concerned stating the occurrence, expected duration and cessation of force majeure, and shall provide evidence of such circumstances.

Failure to notify or untimely notification of force majeure shall deprive an EDF participant of its right to invoke such circumstances.

8. Procedures for use of CIPF

8.1 Types of key media for Siemens DS

The Siemens EDF provides for two types of key media for Siemens digital signature: a hardware-software smart card and a virtual smart card. The use of virtual smart cards is only permitted for Siemens employees.

8.2 Ordering key media for Siemens DS

After signing the Application for Accession, an EDF participant (except for Siemens employees) shall submit to the Authorized EDF Officer a request for issue of a smart card with keys for Siemens DS, using the forms of requests provided in Appendix 4 or 5 hereof.

SIEMENS

The key medium for Siemens DS (physical smart card) is ordered for a Siemens employee in the Human Resource Department as part of the hiring procedure.

To obtain a virtual card, an employee shall file a request on the website: <http://it-services-procurement-tool.siemens.ru>.

A Siemens employee can be issued a smart card and/or a virtual smart card, other participants — a smart card only.

All requests, except for requests from Siemens employees, shall be additionally confirmed by IS.

8.3 Generation of keys for Siemens DS

The keys for Siemens digital are generated together with public key certificate for Siemens digital signature. The keys are generated in a smart card or inside a virtual smart card and shall never used outside it.

8.4 Creation of request for certificate

Based on requests, the administrator of a dedicated LRA computer (CA Registration Authority) creates a request for Participant's certificate using specially generated keys and the LRA administrator's certificate. The Participant's certificate is then sent from the CA to the LRA computer via a secure link. After this, the administrator records the certificate on a smart card. The characteristics of a secure link are provided in the CA Policy.

8.5 Activation of key media for Siemens DS

Regardless of the types of key media for Siemens DS, they are required to be activated before use.

A smart card, or its virtual analogue, once received, shall be activated. This can be done on the website: <https://pkiss-activate-card.siemens.com/>.

Until activated, a card cannot be used for generation of Siemens digital signature as part of a legally relevant document flow.

A card can also be activated by sending an application in English to CA at: operation.trustcenter@siemens.com, stating in the subject line: "Siemens PKI: Card Activation / Aktivierung Ihrer Karte".

8.6 Transportation of smart card

The transportation of a smart card is a process of relocation of a non-activated smart card from the office of Siemens LLC to a point of use, i.e. the office of a legal or natural person (EDF participant).

SIEMENS

An EDF participant (legal person) shall designate a person among its employees to be responsible for the transportation of smart cards, and shall issue a power of attorney for their receipt.

For obtaining smart cards, an EDF participant shall also submit a smart card request (as per the form of Appendix 4 or Appendix 5). The requests are verified and initialed by the human resource function of a legal entity on the overleaf of the application. Requests, together with copies of passports, are forwarded to the Authorized EDF Officer.

8.7 Operation of key media for Siemens DS

An EDF participant, represented by its employees authorized to use a smart card for a legally relevant document flow when exchanging electronic documents with Siemens LLC, shall ensure confidentiality of the keys for Siemens digital signature; shall not make its smart card available to any third party; shall keep the card in a locked safe box; in case of keys loss or compromise, shall notify the CA and IS of the need to revoke the certificates of the compromised Siemens keys.

To notify the CA of the need to revoke the certificate in case of loss or compromise of the keys, it is necessary to approach the CA at: <https://pkiss-emergency.siemens.com/>.

To notify the IS, it is necessary to send a letter, in free form, using the link: digitalsignature.ru@siemens.com.

8.8 Replacement of keys

Using the current keys for Siemens digital signature, a Participant can generate new keys and send a certificate request for a new set of keys.

To block or reissue a card it is necessary to approach the CA using the link: <https://pkiss-emergency.siemens.com/>.

Sending a letter at the above address is always needed if a Participant forgets the PIN code, if a card is lost, or if the PIN code is compromised.

8.9 Decommissioning of key media for Siemens DS

In case of withdrawal from the Siemens EDF, an EDF participant (except for Siemens employees) shall return the smart cards previously issued to it to the Authorized EDF Officer in the office of Siemens LLC within ten (10) working days of such withdrawal.

In case of dismissal of an employee of Siemens LLC, a smart card shall be returned to the Human Resource Department and the public key certificate of the employee will be revoked by the LRA administrator based on a notice of dismissal from the Human Resource Department.

In case of breakdown, replacement of a smart cards user, an EDF participant (except for Siemens employees) shall return the smart card to the Authorized EDF Officer of Siemens LLC

SIEMENS

for maintenance or replacement. The employees Siemens LLC, in case of smart card breakdown shall approach the Human Resource Department for its replacement.

A virtual smart card shall be automatically destroyed in case of dismissal of a respective employee of Siemens LLC, and a public key certificate shall be revoked by the LRA administrator based on a notice of dismissal from the Human Resource Department.

8.10 Requirements for EDF workplaces

A workplace shall conform to the following requirements:

- OC Windows XP (32 Bit) or Windows 7 (64 Bit);
- PKI Basic Client (XP 32Bit) V5.7/PKI Basic Client (Win7 64Bit) V5.7 or higher versions;
- Internet Explorer 7.0 or higher with a “Baltimore CyberTrust Root” CA certificate added to trusted ones (<http://cacert.omniroot.com/bc2025.crt>).

9. Siemens digital signature

9.1 Generation of Siemens digital signature

To generate a Siemens digital signature, the owner of a smart card or virtual smart card shall open a document to be signed, put the smart card in the reader or connect the virtual smart card, complete the authentication procedure and sign the document.

9.2 Procedure for Siemens digital signature verification

The procedure for verifying Siemens digital signature of an EDF participant is described in the current revision of the Certificate Policy of CA of Siemens AG published on the Certification authority’s website: <https://www.siemens.com/pki/>.

To verify Siemens digital signature generated as part of the Siemens EDF it is necessary to install in the OS the CA root certificates available at: https://www.siemens.com/corp/en/index/digital_id/download_siemens_cas.htm

Lists of revoked certificates can be downloaded using the link:

https://www.siemens.com/corp/en/index/digital_id/download_certification_lists.htm

Manual verification of certificates can be performed using the link:

<https://cl.siemens.com/search/basic/>

Validity of certificates issued by the certification authority can be checked at:

<https://dir.ebca.de/>

SIEMENS

To add to trusted websites: <https://pkiss-activate-card.siemens.com/> and <https://pkiss-emergency.siemens.com/>.

After the completion of these steps, the user computer is ready for verifying an enhanced unqualified Siemens digital signature.

To verify Siemens signature under a document, the user shall open the document and click “Verify signature” following the instructions for visualization means suitable for this type of document.

10. Settlement of disputes

The parties to a dispute shall endeavor to amicably resolve all disputes and differences through direct negotiation as part of a claim settlement procedure to their mutual satisfaction. The claim response period is thirty (30) days.

Disputes arising in connection with this electronic document flow Policy (due to accession to this Policy or with regard to the electronic document flow conditions, except for disputes arising in connection with the use of Siemens digital signature) shall be subject to final settlement in a competent Russian court located in Moscow and acting in accordance with the laws of the Russian Federation.

Disputes arising in connection with any processes concerning the lifecycle and/or the use of Siemens digital signature and/or public key certificates for Siemens digital signature issued by the Certification authority of Siemens AG (Germany) shall be subject to final settlement in a competent German court having jurisdiction over the Certification authority of Siemens AG in accordance with the substantive law of the Federal Republic of Germany, without regard to the choice of law principles, and based on the relevant documents of the Certification authority of Siemens AG (including the Certificate Policy of Siemens CA available at: <https://www.siemens.com/pki/>).

11. Key compromise response

Using the valid public keys for Siemens digital signature, an authorized employee of a Participant can generate new keys and send a certificate request for a new set of keys.

To block or reissue a card it is necessary to approach the CA using the link: <https://pkiss-emergency.siemens.com/>

12. Hierarchy of regulatory documents

The main document covering the operating procedures, capabilities and restrictions of an electronic document flow is this EDF Policy and the appendices hereto, developed and applied in accordance with the laws of the Russian Federation (except for the lifecycle and/or the procedures for use of Siemens digital signature).

No transactions, agreements, contracts, applications etc. of EDF participants may conflict with the terms and conditions of this Policy EDF.

The lifecycle and/or the procedures for use of Siemens digital signature are set out in the Policy of the Certification authority of Siemens AG (Germany) and in other documents referred to in clause 13 of this EDF Policy.

The Policy of the Certification authority of Siemens AG (Germany) and its subject matter shall be regulated and construed in accordance with the substantive law of the Federal Republic of Germany, without regard to the choice of law principles, and based on the relevant documents of this certification authority.

In case of conflicts between this EDF Policy and the Policy (and other documents) of the Certification authority of Siemens AG (including the Certification Policy of Siemens CA) published on the website: <https://www.siemens.com/pki/>, the Policy (and other documents) of the Certification authority of Certification authority of Siemens AG (Germany) shall prevail over the EDF Policy.

13. Governing law and jurisdiction

In accordance with this Policy of the Certification authority of Siemens AG (Germany), all processes associated with the lifecycle and/or use of Siemens digital signature shall be governed by the laws and regulations of the Federal Republic of Germany.

In accordance with this Policy, the electronic document flow, procedures for accession to the Policy and implementing electronic document flow (except for the above processes of use of Siemens digital signature) shall be governed by the laws and regulations of the Russian Federation.

Accession to this EDF Policy implies unconditional acceptance of all related documents, including:

1. Provision on the use of unqualified enhanced Siemens digital signature as a part of legally relevant electronic document flow in Siemens LLC (Appendix 7 hereto).

SIEMENS

2. Rules for handling smart cards for EDF participants except for Siemens employees (Appendix 6 hereto).

3. Rules for handling physical and virtual smart cards (for Siemens employees only) (Appendix 8 hereto).

4. Documentation included in the Policy of the Certification authority of Siemens AG (Germany) published on the website: <https://www.siemens.com/pki/>:

4.1 Certificate Policy Siemens CA

4.2 Certification Practice Statement Siemens Root CAs

4.3 Certification Practice Statement Siemens Issuing CAs

4.4 PKI Smart Card Usage for Business-Partners Features and Requirements

4.5 Multipurpose Business Partner Certificates Guideline for the Business Partner

4.6 Siemens Data Privacy Notice

4.7 Binding Corporate Rules (“BCR”) – Summary of Third Party Rights

In accordance with the current laws of the Russian Federation, electronic documents or electronic messages signed with Siemens digital signature of an EDF participant can be used in the Russian Federation as written evidence in a common law or arbitration court, as part of respective relationships with any public and municipal authorities of the Russian Federation (including law enforcement authorities, tax authorities etc.), agencies and institutions (including banks, auditors), or other employees or partners of Siemens.

Appendix 1 - Application for Accession to EDF Policy Siemens LLC (form for legal entities)

Details of corporate applicant	
Full business name of legal entity	
Abbreviated business name of legal entity	
OGRN	
INN	

SIEMENS

Legal address	
Contact details	
Telephone	
E-mail address	
Correspondence address	

_____ (name and form of ownership of organization)
represented by _____ (position)
_____ (full name)
acting under _____

I hereby declare of my accession to the Policy for Siemens Electronic Document Management System registered at: Bolshaya Tatarskaya Str. 9, Moscow 115184 (hereinafter Policy) and acceptance of all the terms and conditions of the Policy in accordance with art. 428 of the Civil Code of Russia, and assume the obligation to observe the provisions of this Policy. I hereby confirm that I was familiarized with the list of risks as per the Policy which arise in the performance of operations using Siemens digital signature and EDF systems. I understand that the list of risks provided in the Policy may not show all possible risks and other aspects of operation of EDF systems and Siemens encryption facilities. I understand and fully accept the risks associated with the use of Siemens encryption facilities and EDF systems.

Director of organization _____
(signature) (full name) _____, 20__

Note of receipt by the authorized EDF officer: ___ h ___ min _____, 20__

Authorized EDF Officer _____
(signature) (full name)

Appendix 2 - Application for Accession to EDF Policy Siemens LLC (form for individuals)

Details of individual applicant	
Last name	
First name	
Patronymic	
Date of birth	
Place of birth	
Permanent residential address	
Identity document	
Type of document	
Series and/or number of document	
Issuing authority	
Issue date	
Contact details	
Telephone	
E-mail address	
Correspondence address	

(last name, first name, patronymic)

I hereby declare of my accession to the Policy for Siemens Electronic Document Management System (hereinafter the Policy) and acceptance of all the terms and conditions of the Policy in accordance with art. 428 of the Civil Code of Russia, and assume the obligation to observe the provisions of this Policy. I agree that over the validity period of this Policy (but for no less than 6 years) Siemens LLC registered at: Bolshaya Tatarskaya Str. 9, Moscow 115184 is entitled to process my personal data provided in this Application and other Applications submitted under the Policy. I acknowledge that the “processing of personal data” for the purposes of this Policy shall mean any action or a combination of actions taken by Siemens LLC as part of this Policy with or without the use of automation facilities, including collection, recording, systematization, accumulation, storage, upgrading, updating, recovery, revision, use, transfer (distribution, provision, access, including cross-border transfer), depersonalization, blocking, deletion, destruction of my personal data in the personal data information systems of Siemens LLC. I confirm that I was explained the meaning of all terms used in this clause and their consistency with Federal Law On Personal Data No. 152-FZ dated 27.07.2006.

I agree that the processing of my personal data provided in this Application and other Applications submitted under the Policy is carried out by Siemens LLC in fulfilling its obligations under the Policy.

Unrestricted

SIEMENS

I was explained that I am entitled to revoke my consent to the processing of my personal data. The request for revocation shall be submitted to Siemens LLC in writing. In case of revoking my consent to personal data processing, Siemens LLC may continue the processing of my personal data without my consent given there are grounds listed in clauses 2 – 11, part 1, article 6, part 2, article 10, and part 2, article 11 of Federal Law On Personal Data No. 152-FZ dated 27.07.2006. I hereby confirm that I was familiarized with the list of risks as per the Policy which arise in the performance of operations using Siemens digital signature and EDF systems. I understand that the list of risks provided in the Policy may not show all possible risks and other aspects of operation of EDF systems and Siemens encryption facilities. I understand and fully accept the risks associated with the use of Siemens encryption facilities and EDF systems.

(signature) (full name) _____, 20__

(completed by the Authorized EDF Officer)

Note of receipt by the authorized EDF officer:

___ h ___ min _____, 20__

Authorized EDF Officer _____
(signature) (full name)

Appendix 3 - Application for Accession to EDF Policy Siemens LLC (form for Siemens employees)

(last name, first name, patronymic)

(series and number of passport, issuing authority and issue date, place of registration)

I hereby declare of my accession to the Policy for Siemens Electronic Document Management System (hereinafter the Policy) and acceptance of all the terms and conditions of the Policy in accordance with art. 428 of the Civil Code of Russia, and assume the obligation to observe the provisions of this Policy. I agree that over the validity period of this Policy (but for no less than 6 years) Siemens LLC registered at: Bolshaya Tatarskaya St. 9, Moscow 115184, is entitled to process my personal data provided in this Application and other Applications submitted under the Policy. I acknowledge that the “processing of personal data” for the purposes of this Policy shall mean any action or a combination of actions taken by Siemens LLC as part of this Policy with or without the use of automation facilities, including collection, recording, systematization, accumulation, storage, upgrading, updating, recovery, revision, use, transfer (distribution, provision, access, including cross-border transfer), depersonalization, blocking, deletion, destruction of my personal data in the information systems of personal data of Siemens LLC. I confirm that I was explained the meaning of all terms used in this clause and their consistency with Federal Law On Personal Data No. 152-FZ dated 27.07.2006.

I agree that the processing of my personal data provided in this Application and other Applications submitted under the Policy is carried out by Siemens LLC in fulfilling its obligations under the Policy.

I was explained that I am entitled to revoke my consent to the processing of my personal data. The request for revocation shall be submitted to Siemens LLC in writing. In case of revoking my consent to personal data processing, Siemens LLC may continue the processing of my personal data without my consent given there are grounds listed in clauses 2 – 11, part 1, article 6, part 2, article 10, and part 2, article 11 of Federal Law On Personal Data No.152-FZ dated 27.07.2006.

I hereby confirm that I was familiarized with the list of risks as per the Policy which arise in the performance of operations using Siemens digital signature and EDF systems. I understand that the list of risks provided in the Policy may not show all possible risks and other aspects of operation of EDF systems and Siemens encryption facilities. I understand and fully accept the risks associated with the use of Siemens encryption facilities and EDF systems.

SIEMENS

(signature)

(full name)

_____, 20__

(completed by the Human Resource Department officer)

Note of receipt by Human Resource Department officer:

___ h ___ min _____, 20__

Human Resource Department _____

(signature)

(full name)

SIEMENS

Appendix 4 - Form of request for issue of smart card (form for legal persons)

1. I request that a smart card and digital certificate for Siemens digital signature be manufactured in accordance with the following identification data:

Name of organization:

Locality:

Region:

Country: RU

Last name, first name, patronymic of the digital certificate owner:

Passport series: _____ number: _____ issued by: _____ issue date: _____

Electronic mail address:

Siemens public key:

Cryptographic facility: CIPF “ _____ ” version _____.

Certificate validity period: three years.

2. In case of a change in the data provided in this request I undertake to immediately inform Siemens LLC of same and submit relevant documents.

3. The owner of Siemens digital certificate hereby grants _____ the right to give instructions on entering data on termination of a Siemens digital certificate into the CA register.

Owner of Siemens digital certificate

(signature) (full name)
Director of organization _____, 20____
(full name) (signature)

(completed by the Authorized EDF Officer)
Note of receipt by the authorized EDF officer: ___ h ___ min _____, 20____

The personal data of the owner of a Siemens digital certificate are accurate:

(signature and full name of the Authorized EDF Officer)
Note of receipt: ___ h ___ min _____, 20____

The Siemens digital signature public verification key is verified.

The Siemens digital signature verification certificate is manufactured.

Appendix 5 - Form of request for issue of smart card (form for individuals)

1. I request that a smart card and digital certificate for Siemens digital signature be manufactured in accordance with the following identification data:

Last name, first name, patronymic of a certificate owner for Siemens digital signature:

Passport series: _____ number: _____ issued by: _____
issue date: _____

Settlement:

Locality:

Country: RU

Electronic mail address:

Siemens public key:

Cryptographic facility: CIPF “_____”version _____.

Certificate validity period: three years.

2. In case of a change in the data provided in this request I undertake to immediately inform Siemens LLC of the same and submit relevant documents.

3. The owner of Siemens digital certificate hereby grants _____ the right to give instructions on entering data on termination of a Siemens digital certificate into the CA register.

Owner of a Siemens digital certificate _____

(signature)

(full name)

(completed by the Authorized EDF Officer)

Note of receipt by the authorized EDF officer:

___ h ___ min _____, 20___

The personal data of the owner of a Siemens digital certificate are accurate:

(signature and full name of the Authorized EDF Officer)

Note of receipt: ___ h ___ min _____, 20___

The Siemens digital signature public verification key is verified.

The Siemens digital signature verification certificate is manufactured.

Appendix 6 - Rules for handling smart cards for EDF participants except for Siemens employees

1. Ordering smart card

After signing the Application for Accession to Policy EDF, an EDF participant sends a request to Siemens LLC for issue of smart cards with verification keys using the request forms in Appendix 4 or 5 of the EDF Policy.

2. Activation of card

A smart card, once received, shall be activated, which can be done at: <https://pkiss-activate-card.siemens.com/>

Until activated, a card cannot be used for generation of Siemens digital signature as a part of a legally relevant document flow.

A card can also be activated by sending an application in English to CA at: operation.trustcenter@siemens.com, stating in the subject line: “Siemens PKI: Card Activation / Aktivierung Ihrer Karte”.

3. Transportation of smart card

An employee of a corporate EDF participant receives smart cards in Siemens LLC after presenting a power of attorney.

4. Operation of card

An EDF participant, represented by its employees authorized to use a smart card for a legally relevant document flow when exchanging electronic documents with Siemens LLC, shall ensure confidentiality of Siemens private keys, shall not make its smart card available to any third party, in case of keys loss or compromise, shall notify the CA and IS of the need to revoke the certificates of the compromised Siemens keys.

To notify the CA of the need to revoke the certificate in case of loss or compromise of the keys, it is necessary to approach the CA at: <https://pkiss-emergency.siemens.com/>.

To notify the IS, it is necessary to send a letter, in free form, using the link: digitalsignature.ru@siemens.com.

5. Replacement of keys

Using the current Siemens private keys, an authorized officer of a Participant can generate new keys and send a certificate request for a new set of keys.

To block or reissue a card it is necessary to approach the CA using the link: <https://pkiss-emergency.siemens.com/>.

SIEMENS

Sending a letter at the above request is always needed if you forget the PIN code of your card, or if you lost your card, or you think somebody could find out the PIN code of your card.

If you lost a card, you should go to the page indicated above and choose a soft (Soft) authentication procedure, which will deliver the form:

Login into the PKI Self Services: Emergency Scenarios

You are in one of the following emergency situations:

- All Corporate ID Card types:
 - You have lost your Corporate ID Card.
 - You have broken your Corporate ID Card.
- Only new type of Corporate ID Card:
 - Your Corporate ID Card has been blocked because you repeatedly entered the wrong PIN.
 - You forgot your PIN.

You can identify the new card type by the imprint "V4.2C" at the lower left corner at the backside of the card

To login to PKI Self Services you need to request a One Time Password. With your One Time Password you can log in exactly one time, within a strictly limited time frame.

Enter your email address as stored in the SCD and click the button "Generate". Your personal One Time Password will be sent to you in an email. With that you can log in immediately.

In case you have already received a One Time Password, you can here login directly.

In this form, you should state your electronic mail address to receive a reference to the authorization page with a one-time password, where you will need to enter your password and electronic mail address.

Please type in your email address and the password that has been sent to you in an email.

Email address:

One Time Password:

After this, the menu window will open listing your actions with your smart card.

Corp. ID Card related
My card is blocked
I have lost my card
I have broken my card

Self management...
I issued PKI keys
I renewed the updating deadline

Certificate management for
A business partner
A functional group
A pseudonym

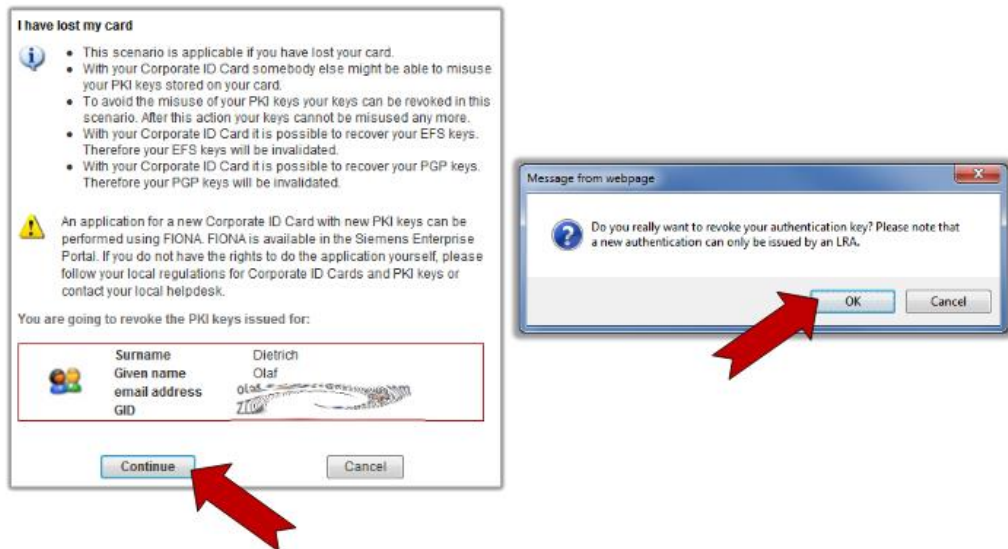
You have logged in with your email address and your Windows password. Therefore, only the functions to be used in case of emergency are available: "I have lost my card" or "I have broken my card". On the left hand side, select the scenario which fits your current situation. You will be guided through these scenarios.

To be able to use the full functionality of PKI Self Services functions log out and log in again using the PKI login. You need your Corporate ID Card to do that.

If you lost your card, choose "I have lost my card"; if your card was broken, choose "I have broken my card".

After this, the following dialogue will appear:

SIEMENS



Where it is necessary to check your data, push the “Continue” button and confirm your choice by push the “Ok” button.

6. Decommissioning

In case of withdrawal from the EDF, an EDF participant shall return the previously issued smart cards of Siemens LLC to the Authorized EDF Officer within ten (10) working days after withdrawal.

In case of breakdown, change of a smart card user, a Participant shall return its smart cards to the Authorized EDF Officer in Siemens LLC for maintenance or replacement.

7. Generation of Siemens private keys

Siemens private keys are generated together with a public key certificate Siemens digital signature.

For EDF participants, requests for Siemens private keys are initiated by the Authorized EDF Officer.

All requests shall additionally be approved by the IS.

8. Generation of Siemens public keys

A public key certificate for Siemens digital signature is generated upon initiation of a smart card.

For EDF participants, requests for a certificate are initiated by the Authorized EDF Officer.

All requests shall additionally be approved by the IS.

Based on requests, the administrator of a dedicated LRA computer creates a certificate request using specially generated keys and the LRA administrator’s certificate. The keys and certificate are forwarded by the CA to the LRA computer via a secure link. After this, the administrator records the keys and certificate on the smart card.

SIEMENS

During the operation of the Siemens CA, the trusted operator ensures that a private CA key remains inside a secure object.

When creating an authentication/digital certificate, a private key is not provided to all participants, because each EDF participant generates its own private key using a device for creating a secure Siemens signature – smart card («SSCD») or software for handling virtual smart cards. For an encryption certificate, a private key is provided to a subject in a secure manner via relevant registration authorities, or by physical transfer of a private key to a subject personally after identity authentication, or by secure postal or courier delivery of a private key following the identity authentication procedure, or through PKISS. For a server certificate, by sending certificate requests in PKCS #10 format, the certificate applicant becomes responsible for confidentiality of a private key. The issuing Siemens CA does not store or generate this key.

9. Obtaining of hardware key medium for Siemens digital signature

An employee of an EDF participant, authorized by the management by issuing a power of attorney, shall obtain smart cards from the Authorized EDF Officer in Siemens LLC against his/her power of attorney and submit them to the relevant department of the Participant.

10. Generation of Siemens digital signature

A user workplace shall conform to the following requirements:

- OC Windows XP (32 Bit) or Windows 7 (64 Bit);
- PKI Basic Client (XP 32Bit) V5.7/PKI Basic Client (Win7 64Bit) V5.7 or higher versions;
- Internet Explorer 7.0 or higher with a “Baltimore CyberTrust Root” CA certificate added to trusted ones (<http://cacert.omniroot.com/bc2025.crt>).

To generate Siemens digital signature, the owner of a smart card shall take the following actions:

- Open a document to be signed.
- Put the smart card in the reader or connect the virtual smart card.
- Push the “Sign the document” button in the application.

The following window will appear:

Smart Card PKI Login



Use Smart Card PKI Login for immediate access to all content.

 Help for Smart Card PKI Login

 login

SIEMENS

Push the “Login” button.

Then enter the PIN code of the card in the below window:



SIEMENS

Appendix 7 - Provision on the use of unqualified enhanced Siemens digital signature as a part of legally relevant electronic document flow in Siemens LLC

1. Goals and subject matter

1.1. This Provision sets out the general procedure and terms for the use of a unqualified enhanced Siemens digital signature (hereinafter Siemens DS) as part of a legally relevant electronic document flow in the Siemens EDM system (hereinafter Siemens EDF), as well as the rights, obligations and the scope of responsibility of EDF participants.

The following terms and definitions are used in this Provision:

- **owner of Siemens digital signature public verification key certificate** – a person duly issued a public verification key certificate for Siemens digital signature. The certificate issue procedure is set out in the EDF Policy. As part of the Siemens EDF, owners of public verification key certificates shall be EDF participants;
- **virtual smart card** – a virtual medium for cryptographic keys, programmable analogue of a physical smart card;
- **document flow** – traffic of documents, from the point of generation or assignment till fulfillment, archiving and (or) dispatch;
- **Siemens digital signature verification public key** – a unique sequence of symbols unambiguously associated with a Siemens private key and designed to verify authenticity of Siemens digital signature (hereinafter also Siemens digital signature verification).
- **Siemens private key** – a unique sequence of symbols designed for generating Siemens digital signature;
- **key information medium** — a physical or logical storage device (smart card, virtual smart card) containing one or more keys for Siemens DS;
- **Siemens public key certificate** – an electronic document or paper document, issued by a certification authority or a representative of a certification authority and confirming the attribution of a Siemens public key to an owner of a Siemens digital signature public verification key certificate;
- **smart card** – a physical medium for Siemens private keys;

SIEMENS

- **Siemens digital encryption facilities** – encryption (cryptographic) facilities used to implement at least one of the following functions: generation of a Siemens digital signature, verification of Siemens digital signature, generation of a Siemens private key and Siemens digital signature public verification key;

- **EDF participant (Business Partner, Siemens employee)** – an individual or legal entity (or an authorized employee of a legal entity), or Siemens employee having acceded the Policy and participating in the electronic document flow;

- **certification authority (CA)** – a legal entity performing the functions of generation and issuance of public verification key certificates for Siemens DS;

- **electronic document** – a document containing information in electronic form;

- **Siemens digital signature (Siemens DS)** – a digital signature used in the Siemens EDF and generated using public key certificates issued exclusively by the CA of Siemens AG. Siemens DS is information configured in electronic form which is connected to other information in electronic form (signed information) or otherwise related to such information and which is used to identify a person signing the information (detail of an electronic document designed to protect an electronic document against forgery and used to identify a public key certificate owner, and to confirm the absence of information distortions in an electronic document). As used in this Policy, this term denotes a unqualified enhanced signature according to Federal Law of Russia On Digital Signature No. FZ-63 dd. 06.04.2011.

1.2. Information in electronic form signed with Siemens DS is considered an electronic document equivalent to a paper document signed in person, except where regulatory instruments require that documents be only executed on paper.

1.3. For the purposes of this Provision, an enhanced unqualified digital signature is Siemens DS which, through the use of a key of an enhanced unqualified Siemens digital signature known solely to an EDF participant (hereinafter a key), proves the fact of generation of a participant's digital signature and allows identifying a Participant (its employee) through the use of a public verification key certificate for Siemens DS.

A key is generated using the software tools of the information system and issued to an EDF participant in accordance with the EDF Policy, which implies the use of Siemens DS in the corporate information system of Siemens LLC as an analogue of a handwritten signature of an EDF participant.

SIEMENS

1.4. A key allows an EDF participant to use the EDF software tools to create Siemens DS and dispatch electronic documents in accordance with the policy of the Certification Authority of Siemens AG and the EDF Policy of Siemens LLC. The parties acknowledge that an electronic document signed with Siemens DS of an EDF participant (having passed the authenticity verification procedure) is considered an outgoing document of an EDF participant. An electronic document signed and dispatched in the EDF contains Siemens DS of an EDF participant and the information evidencing that a document was created and dispatched by an EDF participant.

1.5. Electronic documents are signed by users with the use of hardware devices – secure electronic key information media (smart card) or their programmable analogues – virtual smart cards.

1.6. A document can be signed from any EDF workplace where the Siemens DS software tools are installed.

1.7. To complete the actions required by this Provision, EDF participants shall install and properly adjust the Siemens DS software tools, and shall issue key media and public key certificates Siemens digital signature.

1.8. An EDF participant having signed a document with Siemens DS shall be liable for the contents thereof.

SIEMENS

2. Handling EDF documents with Siemens DS

2.1. EDF participants shall use Siemens DS in accordance with this Provision, EDF Policy of Siemens LLC and the Policy of the CA of Siemens AG.

2.2. When signing a document, the rules for handling smart cards shall be observed.

3. Storage and use of key information media

3.1. A smart card is issued to each EDF participant personally; transfer of a smart card to third parties is prohibited and equated to compromising Siemens private keys.

3.2. The owner of a Siemens public key certificate shall take all reasonable actions to prevent unauthorized access to its key medium.

3.3. When operating with Siemens DS the following is prohibited:

- unauthorized copying of key information media;
- display of Siemens DS keys on the monitor or printer;
- use of key information medium on computers which are not owned by an EDF participant;
- record external files on a key information medium.

3.4. Owners of Siemens DS keys shall be personally liable for security (confidentiality) of Siemens DS keys and shall ensure their integrity, secrecy and non-dissemination.

3.5. The validity period of a public key certificate Siemens DS is three years.

3.6. At least two weeks before expiration of a Siemens DS key, an EDF participant, using the smart card software, shall approach the CA to request for the generation and issuance of a new certificate.

3.7. If a Siemens DS key is compromised (stolen, lost, disclosed, copied without authorization or otherwise may become available to third parties), the owner of a key for Siemens DS shall immediately discontinue its use and forthwith notify the CA.

3.8. Upon dismissal, an employee shall always return his/her smart card with the keys to the Human Resource Department. A virtual smart card shall be blocked with the participation of the system administrator based on a notice of dismissal from the Human Resource Department.

4. Issuance of Siemens digital signature public verification key certificates

4.1. The procedures, rules and obligations of persons participating in the issuance of certificates and encryption facilities for Siemens DS shall be determined in the Policy of CA.

SIEMENS

4.2. Certificates shall be issued upon request for execution and issuance of certificates and encryption facilities for Siemens DS.

5. EDF requirements

5.1. The procedures for gaining access to the EDF are set out in the EDF Policy.

5.2. In case of conflict situations associated with the use of Siemens DS, a commission shall be set up to consider claims of EDF participants, denial of actions with the use of Siemens DS taken by EDF participants, and violations committed when using Siemens DS.

6. Scope of application

6.1. This Provision shall apply to all Siemens EDF participants.

6.2. The fact of familiarization with this Provision shall be confirmed by each EDF participant by acceding to the Siemens EDF Policy.

6.3. The certification authority is the Certification authority of Siemens AG (Germany), which carries out its activities, in particular, issues public key certificates, in accordance with the laws of the Federal Republic of Germany. Siemens private key certificates of EDF participants are generated by the CA of Siemens AG in accordance with the laws of the Federal Republic of Germany and the international standards. In the Russian Federation, this Siemens digital signature fully conforms to all properties of an enhanced encrypted unqualified signature described in Federal Law On Digital Signature No. FZ-63 dd. April 6, 2011 and is recognized an enhanced unqualified signature. The enhanced Siemens digital signature of an EDF participant and electronic documents or electronic messages signed with it have full legal force in the Russian Federation.

6.4. In accordance with the current laws of the Russian Federation, electronic documents or electronic messages signed with Siemens digital signature of an EDF participant can be used in the Russian Federation as written evidence in a common law or arbitration court, as part of respective relationships with any public and municipal authorities of the Russian Federation (including law enforcement authorities, tax authorities etc.), agencies and institutions (including banks, auditors), or other employees or partners of Siemens.

Appendix 8 - Rules for handling physical and virtual smart cards (for Siemens employees only)

1. Ordering smart card

A key medium for Siemens DS (physical smart card) is ordered from an employee of Siemens LLC through the Human Resource Department as a part of the hiring procedure. An employee shall sign the Application for Accession to EDF Policy.

To obtain a virtual card, an employee shall submit an application on the website: <http://it-services-procurement-tool.siemens.ru>.

Information on virtual smart cards is available on the website: <https://intranet.for.siemens.com/wll/0015/en/in/services/clients/Pages/virtualclient.aspx>

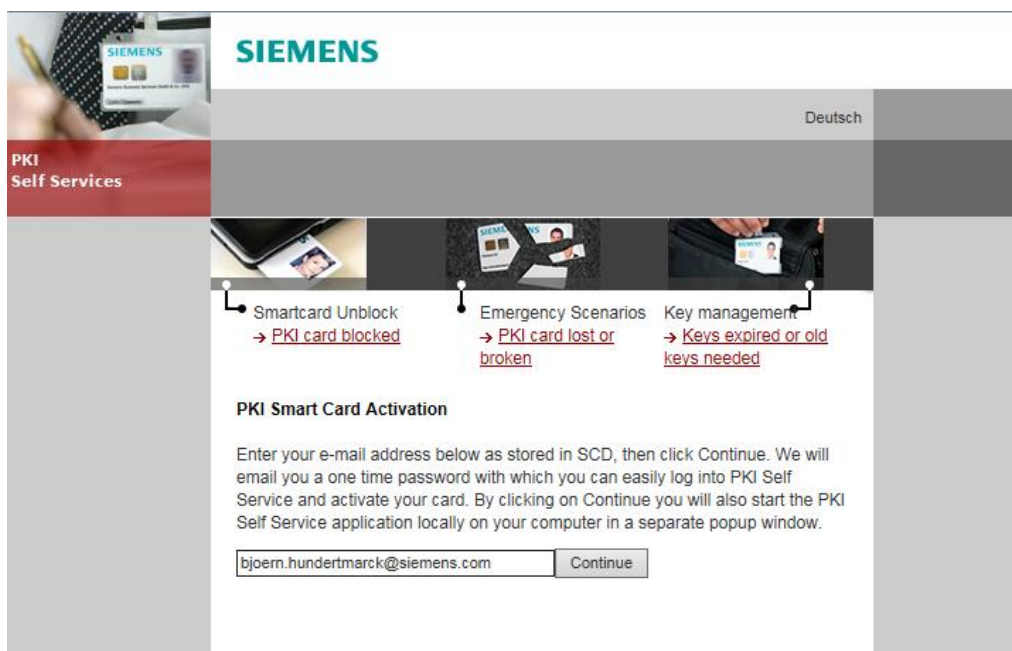
2. Activation of a card

A smart card of any type, once received, shall be activated, which can be done at: <https://pkiss-activate-card.siemens.com/>.

Until activated, a card cannot be used for generation of Siemens digital signature as a part of a legally relevant document flow.

An employee can also activate a card by sending an application in English to CA at: operation.trustcenter@siemens.com, stating in the subject line: “Siemens PKI: Card Activation / Aktivierung Ihrer Karte”.

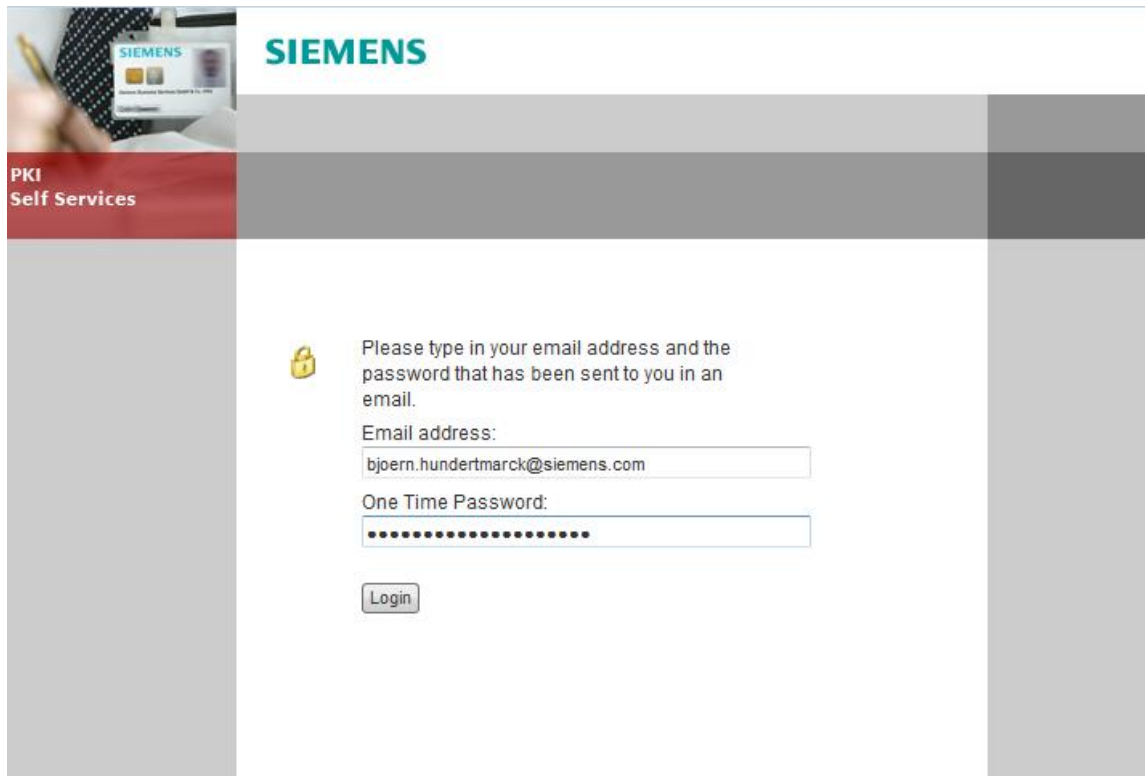
After clicking the link <https://pkiss-activate-card.siemens.com/> you should enter your e-mail address as shown in the picture below.



The screenshot shows the Siemens PKI Self Services website. At the top, there is a navigation bar with the Siemens logo and a language selector set to "Deutsch". Below the navigation bar, there is a red banner with the text "PKI Self Services". The main content area features three columns of links: "Smartcard Unblock -> PKI card blocked", "Emergency Scenarios -> PKI card lost or broken", and "Key management -> Keys expired or old keys needed". Below these links, there is a section titled "PKI Smart Card Activation" with the following text: "Enter your e-mail address below as stored in SCD, then click Continue. We will email you a one time password with which you can easily log into PKI Self Service and activate your card. By clicking on Continue you will also start the PKI Self Service application locally on your computer in a separate popup window." At the bottom of this section, there is an input field containing the email address "bjoern.hundertmarck@siemens.com" and a "Continue" button.

SIEMENS

and push the “Continue” button. As a result of these actions, you will receive at your email address a one-time password which should be entered in the following window.



After this, your card will be activated.

3. Operation of a card

A Siemens employee, when exchanging electronic documents with other EDF participants, shall ensure confidentiality of Siemens private keys, shall not make its smart card available to any third party, in case of keys loss or compromise, shall notify the Certification Authority of Siemens AG of the need to revoke the certificates of the compromised Siemens keys.

4. Replacement of keys

Using the current Siemens private keys, an employee of Siemens LLC can generate new keys and send a certificate request for a new set of keys.

To block or reissue a card of any type it is necessary to approach the CA using the link: <https://pkiss-emergency.siemens.com/>.

A card can be blocked by both an employee as well as the representatives of the Human Resource Department, as well as the LRA administrator.

Sending a letter at the above address is always needed if you forget the PIN code of your card, or if you lost your card, or you think somebody could find out the PIN code of your card.

If you lost a card, you should go to the page indicated above and choose a soft (Soft) authentication procedure, which will deliver the form:

Login into the PKI Self Services: Emergency Scenarios

You are in one of the following emergency situations:

- All Corporate ID Card types:
 - You have lost your Corporate ID Card.
 - You have broken your Corporate ID Card.
- Only new type of Corporate ID Card:
 - Your Corporate ID Card has been blocked because you repeatedly entered the wrong PIN.
 - You forgot your PIN.

You can identify the new card type by the imprint "V4.2C" at the lower left corner at the backside of the card

To login to PKI Self Services you need to request a One Time Password. With your One Time Password you can log in exactly one time, within a strictly limited time frame.

Enter your email address as stored in the SCD and click the button "Generate". Your personal One Time Password will be sent to you in an email. With that you can log in immediately.

In case you have already received a One Time Password, you can here login directly.

In this form, you should state your electronic mail address to receive a reference to the authorization page with a one-time password, where you will need to enter your password and electronic mail address.

Please type in your email address and the password that has been sent to you in an email.

Email address:

One Time Password:

After this, the menu window will open listing your actions with your smart card.

Please wait while information about your current key inventory will be retrieved from the Siemens Trust Center. This page will be refreshed automatically.

Corp. ID Card related

- My card is blocked
- I have lost my card**
- I have broken my card

Self management...

- I read PKI keys
- I missed the updating deadline

Certificate management for

- A business partner
- A functional group
- A pseudonym

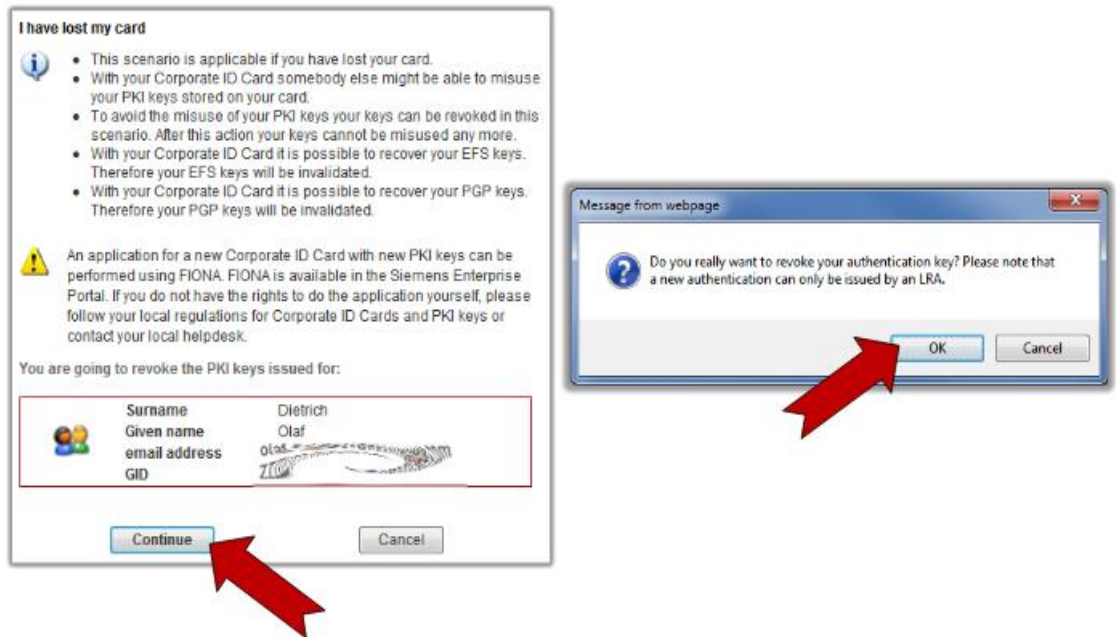
You have logged in with your email address and your Windows password. Therefore, only the functions to be used in case of emergency are available. "I have lost my card" or "I have broken my card". On the left hand side, select the scenario which fits your current situation. You will be guided through these scenarios.

To be able to use the full functionality of PKI Self Services functions log out and log in again using the PKI login. You need your Corporate ID Card to do that.

If you lost your card, choose "I have lost my card"; if your card was broken, choose "I have broken my card".

After this, the following dialogue will appear:

SIEMENS



Where it is necessary to check your data, push the “Continue” button and confirm your choice by push the “Ok” button.

5. Decommissioning

In case of breakdown, an employee shall return the smart cards to the Human Resource Department of Siemens LLC for maintenance or replacement.

A virtual smart card shall be blocked with the participation of the system administrator based on a notice of dismissal from the Human Resource Department.

Upon dismissal, an employee shall always return his/her physical smart card to the Human Resource Department.

6. Generation of Siemens private keys

Siemens private keys are generated together with a public key certificate Siemens digital signature.

A key request is generated automatically in the Fiona system.

7. Generation of Siemens digital signature public keys

A public key certificate for Siemens digital signature is generated upon initiation of a physical and virtual smart card of an employee.

A request for a public key certificate Siemens DS shall be initiated by a Human Resource Department officer in the Fiona system.

Based on requests, the administrator of a dedicated LRA computer creates a certificate request using specially generated keys and the LRA administrator’s certificate. The keys and certificate are forwarded by the CA to the LRA computer via a secure link. After this, the administrator records the keys and certificate on the smart card of any type.

SIEMENS

During the operation of the Siemens CA, the administrator ensures that a private CA key remains inside a secure object.

When creating an authentication/digital certificate, a private key is not provided to all participants, because each EDF participant generates its own private key using a device for creating a secure Siemens signature – smart card («SSCD») or software for handling virtual smart cards. For an encryption certificate, a private key is provided to a subject in a secure manner via relevant registration authorities, or by physical transfer of a private key to a subject personally after identity authentication, or by secure postal or courier delivery of a private key following the identity authentication procedure, or through PKISS. For a server certificate, by sending certificate requests in PKCS #10 format, the certificate applicant becomes responsible for confidentiality of a private key. The issuing Siemens CA does not store or generate this key

8. Obtaining of Siemens private key medium

To obtain a physical smart card containing a verification key and public key certificate for Siemens digital signature, an employee shall refer to the Human Resource Department.

To obtain a virtual smart card, an employee shall install the necessary software available for downloading at: <https://www.siemens.com/nscinstaller>.

After software installation, an employee shall run the software, generate keys using the software, and create a certificate request. The certificate request shall be sent to the LRA administrator.

Once issued, a certificate shall be installed on a virtual smart card.

Employees of Siemens LLC being EDF participants shall maintain confidentiality of Siemens private keys, shall not make their smart card available to third parties, in case of keys loss or compromise, shall notify the CA and IS of the need to revoke the certificates of the compromised Siemens keys. To notify the IS and CA of a violation, a letter in free form shall be sent at the following addresses: for IS - digitalsignature.ru@siemens.com, for CA - <https://pkiss-emergency.siemens.com/>, and the following actions shall be taken:

Login into the PKI Self Services: Emergency Scenarios

You are in one of the following emergency situations:

- All Corporate ID Card types:
 - You have lost your Corporate ID Card.
 - You have broken your Corporate ID Card.
- Only new type of Corporate ID Card:
 - Your Corporate ID Card has been blocked because you repeatedly entered the wrong PIN.
 - You forgot your PIN.

You can identify the new card type by the imprint "V4.2C" at the lower left corner at the backside of the card

To login to PKI Self Services you need to request a One Time Password. With your One Time Password you can log in exactly one time, within a strictly limited time frame.

Enter your email address as stored in the SCD and click the button "Generate". Your personal One Time Password will be sent to you in an email. With that you can log in immediately.

In case you have already received a One Time Password, you can here login directly.

Please type in your email address and the password that has been sent to you in an email.

Email address:

One Time Password:

Please wait while information about your current key inventory will be retrieved from the Siemens Trust Center. This page will be refreshed automatically.

■■■■■

Corp. ID Card related
My card is blocked
I have lost my card
I have broken my card

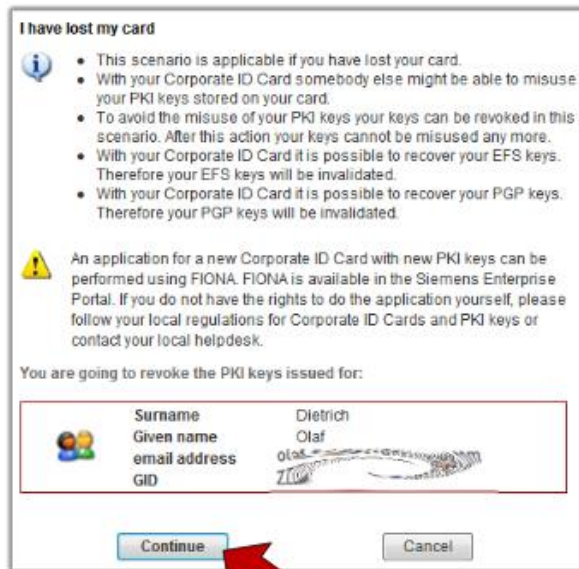
Self management...
I missed PKI keys
I missed the updating deadline

Certificate management for
A business partner
A functional group
A pseudonym

You have logged in with your email address and your Windows password. Therefore, only the functions to be used in case of emergency are available: "I have lost my card" or "I have broken my card". On the left hand side, select the scenario which fits your current situation. You will be guided through these scenarios.

To be able to use the full functionality of PKI Self Services functions log out and log in again using the PKI login. You need your Corporate ID Card to do that.

SIEMENS



9. Generation of Siemens digital signature

A workplace of an employee of Siemens LLC being EDF participant shall conform to the following requirements:

- OC Windows XP (32 Bit), Windows 7 (64 Bit) or Windows 10 (64 Bit);
- PKI Basic Client (XP 32Bit) V5.7/PKI Basic Client (Win7 64Bit) V5.7 or higher versions;
- Internet Explorer 7.0 with a “Baltimore CyberTrust Root” CA certificate added to trusted ones (<http://cacert.omniroot.com/bc2025.crt>).

To generate Siemens digital signature, the owner of a smart card shall take the following actions:

- Open a document to be signed.
- Put the smart card in the reader or connect the virtual smart card (by right-clicking the gray cloud icon on the task bar and choose “Insert Network Smart Card”).




- Push the “Sign the document” button in the application.

The following window will appear:

Smart Card PKI Login

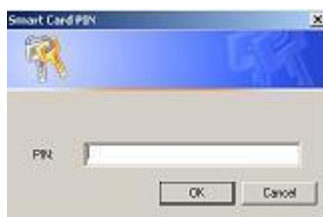


Use Smart Card PKI Login for immediate access to all content.

 Help for Smart Card PKI Login

Push the “Login” button.

Then enter the PIN code of the card in the below window:

A screenshot of a Windows-style dialog box titled "Smart Card PIN". The dialog box has a blue header bar with a key icon on the left. Below the header, there is a text input field labeled "PIN". At the bottom of the dialog box, there are two buttons: "OK" and "Cancel".

Appendix 9 – License of EDF Operator issued to Siemens LLC by the FSS

Центр по лицензированию, сертификации и защите
государственной тайны ФСБ России
(наименование лицензирующего органа)

ЛИЦЕНЗИЯ

ЛСЗ № 0014454 * Рег. № 15891 Н от « 14 » апреля 2017 г.

На осуществление (указывается лицензируемый вид деятельности) разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)

Виды работ (услуг), выполняемых (оказываемых) в составе лицензируемого вида деятельности, в соответствии с частью 2 статьи 12 Федерального закона «О лицензировании отдельных видов деятельности» (указываются в соответствии с перечнем работ (услуг), установленным положением о лицензировании соответствующего вида деятельности):
работы, предусмотренные пунктами 12, 13, 14, 17, 18, 20, 21, 22, 23 перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, являющегося приложением к Положению, утвержденному постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313.

Настоящая лицензия предоставлена (указывается полное и (в случае, если имеется) сокращенное наименование (в том числе фирменное наименование), организационно-правовая форма юридического лица, фамилия, имя и (в случае, если имеется) отчество индивидуального предпринимателя, наименование и реквизиты документа, удостоверяющего его личность)
обществу с ограниченной ответственностью «Сименс» (ООО «Сименс»)

Основной государственный регистрационный номер юридического лица (индивидуального предпринимателя) (ОГРН) 1027739473739
Идентификационный номер налогоплательщика 7725025502

