

## GENERAL TERMS AND CONDITIONS

### on digital Certificates

#### A. Certification Services

##### 1. Certification

###### 1.1 Certification of Public Keys

1.1.1 Provider carries out the certification of public keys in accordance with the current certification guidelines of the respective certification authority, which can be retrieved in the internet under <http://www.trustcenter.de/repository>

1.1.2 With the application for a certificate, the customer gives his consent to the issuance of a certificate for him, which according to the service description of this certificate may be added to Provider's directory of certificates and therefore made publicly available.

1.1.3 An application for certification can only be carried out once all the necessary information is available. Provider reserves its right to reject an application for certification.

1.1.4 As long as Provider has informed the customer when they apply for a certificate about any restrictions, Provider is entitled to include a statement about a restriction of use in the certificate.

###### 1.2 Scope of Certification

Only statements made by the applicant in the course of applying for a certificate will be checked by Provider when issuing the certificate.

###### 1.3 Utilization of Certificates

If the certificate is a Server Certificate or WildCard Certificate this certificate is only allowed to be used for the agreed upon number of servers and only for this number of physical servers. It is prohibited to use this certificate on more than the agreed number of servers at the same time. It is prohibited to use this Server Certificate for or on behalf of any other organization. It is prohibited to perform private or public key operations in connection with any domain name or organization name other than the name submitted during enrolment. The use of TC Publisher ID for Adobe AIR in connection with MS Authenticode or Java Desktop Code Signing is not allowed.

#### 2 Directory Services

##### 2.1 Certificate Requests

2.1.1 Once a certificate is added to the public directory service, anyone can search for individual certificates in the directory of certificates.

2.1.2 Certificates which have been revoked will be made available to the public by via certificate revocation lists (CRL) and where appropriate via the directory of certificates of the respective certification authority.

##### 2.2 Transmission of Data

2.2.1 Provider's directory of certificates transmits the data stated in the certificate automatically to all who access it. This transmission is carried out globally. Only the information about persons or organisations contained in the certificate as well as the status of the certificate will be submitted.

2.2.2 Provider will only obtain, process and utilise the personal and organisation-related data which is necessary for the issuance of a certificate and the listing of that certificate in the directory of certificates.

2.2.3 Provider will not transmit the data contained in certificates to third parties for advertising purposes. Provider will only assign the processing of data to companies, which operate compliant to the applicable data protection laws.

2.2.4 Provider undertakes to keep all personal and organisation-related data which is not included in the certificate secure from unauthorised access. Provider reserves its right to mention an organisation as a customer.

#### 3 Revocation of Certificates

##### 3.1 Reasons for Revocation

3.1.1 The owner of a certificate shall be obliged to revoke its certificate if

(a) any of the reasons set out in clause 4.1 of these General Terms and Conditions take place, or

(b) a certificate has been issued in relation to an organisation and the owner of that certificate has left the organisation.

3.1.2 In the event that Provider becomes aware of any of the reasons mentioned in clause 3.1.1 of these General Terms and Conditions without the owner of the certificate having previously arranged for the certificate to be revoked, then Provider may revoke the certificate itself.

3.1.3 Furthermore, Provider is entitled to revoke a certificate if

(a) there is any indication or evidence of the trustworthiness or the security functions of the certificate having been broken due to negligence or carelessness in complying with the duties of care and support mentioned in paragraph 4 of these General Terms and Conditions,

(b) the basic algorithm of the certificate is deciphered,

(c) the customer is substantially overdue with any payments required for the services of Provider.

##### 3.2 Means of Revocation

3.2.1 The certificate may be revoked

(a) at the website of Provider at <http://www.trustcenter.de/revoke>,

(b) by signed e-mail to [certificate@trustcenter.de](mailto:certificate@trustcenter.de) or [certificate@chosensecurity.com](mailto:certificate@chosensecurity.com)

(c) by telephone call with revocation password to +49 (0)40/80 80 26-1 13 (Germany) or 1-800-468-2180 (toll free - USA)

(d) by writing to Provider, subject "Revocation", TC TrustCenter GmbH, Sonninstrasse 24-28, 20097 Hamburg, Germany, or ChosenSecurity, Inc., 1000 Highland Avenue, Suite 200, Needham, MA 02494 USA.

The above addresses and telephone numbers shall be used exclusively for revocation. No help or assistance can be given under the above contacts.

3.2.2 The owner of the certificate hereby authorises Provider to record any telephone conversations made for revocation purposes. In the event that the owner of the certificate arranges for a third party to telephone the Provider for matters of revocation, then the third party shall be informed by the owner of the certificate of that authorisation.

#### B Obligations of the Customer

##### 4 Obligations of Care and Co-operation of the Owner of the Certificate

The following obligations are core contractual obligations of the owner of the certificate.

4.1 The media containing the data with the private key shall be secured personally. In the event of any loss the revocation of the certificate shall be arranged at once. If the media containing the private key are no longer required they shall be rendered unusable and the revocation of the certificate shall be arranged in the event that it is not yet expired. Similarly, the owner of the certificate shall arrange a revocation of the certificate if any data contained in the certificate no longer conforms with the facts or is no longer conformant with the data made available at the time of certification or the certificate holder has knowledge or the suspicion that his/her private key has been compromised or used by an unauthorized party.

4.2 Personal identification numbers or passwords for identification in relation to the data media containing the private key shall remain secret. In particular, they shall not be noted or marked on the related media or in any other way stored together with such media. In the event of release or the suspicion of the release of such identification information, the information shall be changed at once or a revocation shall be arranged.

4.3 It must be ensured that no virus or potentially damaging software is used or stored on any hardware which could lead to the revelation of the identification data or the private key, or which could allow the signature or signature verification procedures to be compromised or copied.

4.4 In order to achieve optimal security in the verification of digital signatures it is necessary to check in the certificate directory of Provider or other certification authorities whether or not the signature key certificates of the authority are valid and not revoked.

4.5 Every owner of a certificate shall select a revocation password for the revocation of this certificate. This revocation password should be available for use in emergencies and protected against misuse by third parties. Provider hereby puts the Customer on notice that the misuse of the revocation password can in particular cases lead to considerable damage.

4.6 The customer will only let his own name be certified by Provider. Own names are those on which no third parties, especially other customers or other organisations, have rights or entitlements.

## **C Diversification of Risks**

### **5 Liability**

5.1 Provider shall be liable for intent and gross negligence. In slight negligence cases of imputable damages due to personal injury, Provider shall be liable without limitation.

5.2 In the event of the violation of material contractual obligations, Provider shall be liable for slight negligence, but limited to the typical contractual direct average damage, foreseeable for Provider. This also applies for slight negligent violation of obligations of vicarious agents of Provider.

5.3 Provider shall not be liable for acts of the owner of a certificate or third parties that use a certificate in an unauthorized way, for their legal capabilities, their solvency, or for the validity of the agreement made by using the keys.

5.4 Provider shall not be liable for failures which are not within Provider's scope of responsibility, especially for technical failures or non availability of the certificate directory or single certificates.

5.5 Provider shall not be liable for the security of the public key security systems of the customer as far as these are not purchased from Provider.

5.6 Provider shall not be liable for the loss of data and/or programs if the damage is due to the fact that the customer has not run data back-up in order to ensure that lost data can be recovered with reasonable efforts.

5.7 The customer shall immediately inform Provider about any damages or losses, which entitles the customer to claims against Provider.

### **6 Warranty**

6.1 The customer is obliged to check all statements in the certificate for incompleteness and incorrectness, and must notify the Provider immediately if any are found, following the fulfilment of the service by Provider.

6.2 Provider will replace a defective certificate by issuing a new certificate if the defect is caused by Provider. It should be noted that a defective certificate will be revoked and cannot be used anymore.

6.3 The customer shall inform Provider, in writing, within a period of two weeks from the reception of the goods, or a certificate, of recognisable defects; otherwise a warranty claim is void. Hidden defects shall be communicated in writing immediately after their detection. In order to be within the term, the notice needs to be dispatched in due time. It is the obligation of the customer to prove all conditions of entitlement of a warranty claim, especially for the defect itself, for the time required to recognize the error and the timeliness of the defect notification.

6.4 Provider will meet its warranty obligations primary by remedy of the defect or additional delivery, at the choice of Provider.

6.5 In the event that the remedy of the defect fails, the customer may, at its own discretion, demand reduction of the payment or rescind the contract. In the case of only slight deviations from the contract, especially in the event of minor defects, the customer may not rescind the contract.

6.6 If the customer chooses to rescind the contract after unsuccessful attempts to remedy the defect, in the event of a defect of the goods or the title, the customer may not claim any damages.

If the customer claims damages after unsuccessful remedy of the defect, the goods remain with the customer. The claim shall be limited to the difference between the purchase price and the value of the defective goods. This does not apply in the event that Provider has committed the breach maliciously.

6.7 The term of warranty is one year starting from the delivery of the goods. If the customer has not notified Provider of the defect in due time, no warranty term is applicable.

6.8 If the customer receives defective documentation, Provider shall deliver the documentation free of defects. This applies only if the defect in the documentation prevents the proper use.

6.9 The customer receives no guarantees in the legal terms from Provider. In particular, due to the high amount of available applications (e.g. internet browsers) Provider cannot make any statements about compatibility of certificates with these applications.

6.10 If the Provider cannot fulfil its contractual obligation at all or on time due to force majeure, strike, war, riots or other events beyond the Provider's control, Provider cannot be held liable in any way.

### **7 Passing of Risk**

The risk of incidental loss or incidental deterioration will be passed on to the customer with delivery of the goods to the party responsible for delivering the goods. If the delivery is being held up by demand of the customer, the risk will be passed on to the customer once the goods have been declared ready for delivery.

### **8 Retention of Title**

8.1 The title of the delivered goods remains with Provider until settlement of all claims of Provider within the ongoing business relationship with the customer. The customer is under an obligation to treat the delivered goods with reasonable care.

8.2 The customer is under an obligation to inform Provider immediately in the event that the goods are subject to garnishment as well as in the event of damage or destruction of the goods. The customer shall notify Provider of any change of ownership of the goods as well as any change of the registered business address of the customer.

8.3 Provider is entitled to withdraw from the contract and reclaim the delivered goods in the event of any breach of contract by the customer, especially for any delayed payment or breach of a contractual obligation as stated in clause 8.2 of these General Terms and Conditions.

## **9 Export**

Any export of hardware or software with encryption capabilities by Provider shall be subject to the condition that permission is obtained from the responsible authorities at the time of the export. In the event that any necessary export permit is refused Provider shall be entitled to withdraw from the contract. There shall be no valid claims for damages resulting from any delay related to the procedures for obtaining an export permit.

## **D Contractual Relationship**

### **10 Scope**

10.1 The services described in these General Terms and Conditions are not subject to the German Signature Act. Only certificates expressly mentioned as "qualified certificates" in the relevant service description can be used to create a qualified electronic signature.

10.2 Deviating, opposing or supplementary general terms and conditions will not form part of the contract even in the event that these are known to the Provider, unless Provider clearly agrees to those in writing.

10.3 The law of the Federal Republic of Germany is applicable for these General Terms and Conditions, expressly excluding international private law and the UN Treaty on International Sale of Goods.

10.4 The customer shall be notified in writing of any modification of these General Terms and Conditions. Such modifications are deemed to be accepted if the customer does not object to them in writing. Provider will point out this consequence in particular. The customer must inform Provider within six weeks in writing after notification of modification in the event that the customer objects to the modification.

10.5 The invalidity of one or more provisions of these General Terms and Conditions shall not affect the validity of the remaining provisions of these General Terms and Conditions.

10.6 A certificate which is issued royalty-free may not be commercially used. Provider grants no warranty and provides no maintenance or support for royalty-free services.

### **11 Conclusion of Contract**

11.1 For American, Asian and Australian customers the contracting party on Provider's site will be:

ChosenSecurity Inc., 1000 Highland Ave., Suite 200, Needham, MA 02492, USA

For European and African customers the contracting party on Provider's site will be:

TC TrustCenter GmbH, Sonninstrasse 24 – 28, 20097 Hamburg, Germany

11.2 The services and offers of Provider are solely based on these General Terms and Conditions which shall also apply, without having been specifically agreed again, to all future business.

11.3 All details in brochures, advertisements or equivalent on the services of Provider also including prices are non binding and subject to confirmation in writing. Technical modifications are acceptable within reasonable limits.

11.4 Provider is entitled to accept the proposal to enter into an agreement included in the order within two weeks after receipt. The acceptance of the proposal to enter an agreement may take place in writing or in performance of the service.

11.5 When a certificate is to be transferred onto a signature card, the fulfilment of the contract shall be under the condition of the proper and timely delivery by the supplier of Provider. This does not apply in the event that the non-delivery is not caused by Provider, especially when signing a congruent hedging transaction.

The customer will be informed without unreasonable delay about the non-availability of the service. Invoices paid will be refunded.

11.6 If the service has been ordered from Provider's websites, the agreement will be saved by Provider and, upon request, will be sent to the customer along with these Terms and Conditions via email.

### **12 Place of Jurisdiction and Written Form**

12.1 In so far as the customer is a business customer, or if the customer is a public corporation or public asset, the exclusive place of jurisdiction for all legal disputes arising from or in connection with this agreement is Boston for customers of ChosenSecurity or Hamburg for customers of TC TrustCenter.

12.2 All modifications or supplements of contractual agreements shall be made in writing for evidence purposes. This also applies for the requirement of the written form itself. The requirement for the written form shall be adhered to by utilising the digitally signed form.

12.3 These General Terms and Conditions are a translation of the German version of our General Terms and Conditions. In the event of lack of clarity or questions with regard to the interpretation of these General Terms and Conditions, the original and authoritative German version shall prevail.

## **E Termination of the Contract**

### **13 Termination**

13.1 The term of the contract is bound to the validity term of the certificate. Due to the fact that the certificate must be listed in the certificate directory after revocation, no paid money can be refunded after termination or cancellation of the contract.

13.2 Provider is entitled to terminate the contract in writing in the event that Provider becomes aware of the fact that the customer has made false statements about his creditworthiness.

13.3 Provider is furthermore entitled to terminate the contract if the credit rating has declined since entering the contract, especially in an event of protested bills or if an insolvency petition has been filed.

13.4 A termination becomes effective after a period of one month. Provider will execute the termination by revoking the certificate.

13.5 The right for an extraordinary termination remains unaffected hereby.

## **F Terms of Payment**

### **14 Prices**

14.1 All prices stated by Provider are exclusive of value added tax, which will be added at the applicable rate.

14.2 In the event that the period from the date of the formation of the contract to the agreed date of performance or delivery of goods or the date of performance or delivery of goods desired by the customer and accepted by Provider exceeds 4 months, the prices on the date of performance or delivery shall apply. If the prices agreed to in the contract are exceeded by more than 10 per cent, the customer shall be entitled to terminate the contract.

### **15 Payment**

15.1 Invoices amounts are due within 14 days from the date of the invoice.

15.2 The contractual parties may only deduct from claims which are legally final or undisputed.

15.3 In the event that the Customer is in default with payment, Provider may demand interest from the start of the default not less than eight percent per year above the statutory interest rates. Furthermore, Provider reserves the right to make further claims based on damage resulting from default.

15.4 Should a customer persistently exceed the payment term agreed with Provider, this will entitle Provider to deliver services in future only in return for the provision of collateral or payment three months in advance. This also applies in the instance of deterioration of the creditworthiness of the customer, especially if an insolvency petition has been filed.

15.5 The assignment of claims is only allowed with the prior written approval of the other party to the contract, which shall not be unreasonably denied. A right of retention is only valid for opposite claims of the respective contractual agreement.

## **F Terms on Special Distributions**

### **16 Coupon Codes**

16.1 If a customer orders more than one certificate Provider will give the customer a list of coupon codes. Using a coupon code the customer is able to request a single certificate

16.2 The coupon codes have a validity of 12 months since issuance of the coupon code list. After the validity date, not used coupon codes expire unless the customer undertakes a re-order. The amount of the re-order shall not go below of 50 per cent of the remaining quantity of the not used coupon codes. The re-order must correspond to the same certificate product like the initial order.

16.3 The assignment and especially the resale of a coupon code is not allowed. By using coupon codes the customer is only entitled to request certificates for the customer itself. In this meaning, a customer is exclusively the contracting party and in no event an affiliate. By request of the customer the Provider will send the customer the initially transmitted coupon code list again.

### **17 TC ID Store**

17.1 If the customer orders a TC ID Store, Section 16 above regarding Coupon Codes shall not apply.

17.2 Notwithstanding Clause 11.4, parties will enter into the agreement by written confirmation of the order via an e-mail containing access data.

17.3 In addition to Clause 15, the customer shall pay a start deposit at the commencement of the agreement term. The term during which certificates can be ordered from the deposit (the Order Term) shall be two years from the commencement of the agreement or until such time as the deposit is exhausted, whichever occurs first. The agreement term shall terminate on the date of the expiration of the validity term of the last certificate.

17.4 Notwithstanding Clause 13.4 a TC ID Store cannot be terminated. The customer may enter into a new agreement on a TC ID Store with a new Order Term. If the parties enter into such a subsequent agreement and the customer has a remaining deposit in an existing TC ID Store, the remaining deposit may be credited to the subsequent agreement if the remaining deposit has less than the value of the highest certificate price of product in the TC ID Store or if this credit does not exceed half of the initially contracted deposit.

If the parties have not entered into a new agreement at the end an agreement term, any remaining deposit of the customer will be not credited back to the customer.

17.5 In addition to Clause 4 the following obligations shall apply. The customer shall:

(a) observe the duties contained in the TC TrustCenter Certification Guidelines;

(b) submit only vetted, correct certificate details to TC TrustCenter and in the case that Provider sends customer the certificate details, after receipt of the certificate confirm the accuracy of such details in the certificate). Written notice of incomplete and incorrect details as well as recognisable defects shall be provided immediately after fulfilment of performance and hidden defects immediately after detection;

(c) ensure that a least one administrator for the TC ID Store is appointed during the term of the agreement;

(d) appoint only administrators for the TC ID Store which are duly authorized to register and add users, modify users and user roles, delete users, revoke, suspend and unsuspend certificates, and initiate key recovery for recoverable certificates, or take similar actions. The appointed administrators must be obliged to fulfill the requirement of to lit. (a) above as well as to keep the personal access data confidential.

(e) use the TC Business ID for Adobe certificates – as far as this is part of the provided service – in compliance with all applicable laws and regulations including without limitations US export laws and regulations..

17.6 Notwithstanding Clause 3.2.1, a certificate may be revoked within the TC ID Store solely by the certificate holder or by the administrator of the TC ID Store.

17.7 The Parties shall comply with all applicable data protection laws and regulations, including by ensuring that their technical facilities are in compliance therewith and that their employees are informed of and comply with such legal obligations.

To the extent that personal data is created in connection with the services, the customer shall ensure that any collection, processing and use of personal data is in accordance with applicable law. To the extent that the customer makes available any personal data, the customer warrants that the data has been legally collected and processed and used for the intended purpose and that it may be made available to the Provider. The Provider shall collect, process and use the personal data only to the extent necessary for the performance of the agreement. The Provider shall not be obliged to verify the legality of the collection, processing or use of the data. The customer shall indemnify the Provider against any claims by third parties resulting from the collection, processing or use of personal data. The above indemnification shall include the costs of any legal defence.

– END OF DOCUMENT –