

Chosen Security™ and TC TrustCenter Certificate Policy and Certification Practice Statement for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

NOTE: The information contained in this document is the property of Chosen Security, Inc.. This Certification Practice Statement and Certificate Policy is published in conformance with international practices (see [RFC2527]).

This document may not be copied, distributed, used, stored or transmitted in any form or by any means, whether in part or as a whole, without the prior written consent of Chosen Security, Inc..

Copyright 2007 by Chosen Security, Inc.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

1	INTRODUCTION	5
1.1	OVERVIEW	5
1.2	IDENTIFICATION	6
1.3	COMMUNITY AND APPLICABILITY	6
1.3.1	<i>Certification authorities</i>	7
1.3.2	<i>Registration authorities</i>	7
1.3.3	<i>End entities</i>	7
1.3.4	<i>Applicability</i>	7
1.4	CONTACT DETAILS	7
	<i>Specification administration organization</i>	7
	<i>Contact person</i>	8
2	GENERAL PROVISIONS	9
2.1	OBLIGATIONS	9
2.1.1	<i>CA obligations</i>	9
2.1.2	<i>RA obligations</i>	9
2.1.3	<i>Subscriber obligations</i>	10
2.1.4	<i>Relying Party obligations</i>	10
2.1.5	<i>Repository obligations</i>	10
2.1.6	<i>Certificate Revocation and Renewal</i>	11
2.2	LIABILITY	11
2.2.1	<i>Limited Warranty/Disclaimer</i>	11
2.2.2	<i>Limitation on Liability</i>	12
2.3	FINANCIAL RESPONSIBILITY	13
2.3.1	<i>Insurance</i>	13
2.3.2	<i>Indemnification by Relying Parties and Subscribers</i>	13
2.3.3	<i>Fiduciary relationships</i>	13
2.4	INTERPRETATION AND ENFORCEMENT	14
2.4.1	<i>Governing law</i>	14
2.4.2	<i>Severability, survival, merger, notice</i>	14
2.4.2.1	<i>Severability</i>	14
2.4.2.2	<i>Survival</i>	14
2.4.2.3	<i>Merger</i>	14
2.4.2.4	<i>Notice</i>	14
2.4.3	<i>Dispute resolution procedures</i>	14
2.5	FEEs	15
2.6	PUBLICATION AND REPOSITORY	15
2.6.1	<i>Publication of CA information</i>	15
2.6.2	<i>Frequency of publication</i>	15
2.6.3	<i>Access controls</i>	15
2.6.4	<i>Repositories</i>	15
2.7	COMPLIANCE AUDIT	15
2.8	CONFIDENTIALITY	16
2.9	INTELLECTUAL PROPERTY RIGHTS	16
3	IDENTIFICATION AND AUTHENTICATION	17
3.1	INITIAL REGISTRATION	17
3.1.1	<i>Types of names</i>	17
3.1.2	<i>Need for names to be meaningful</i>	17
3.1.3	<i>Rules for interpreting various name forms</i>	17
3.1.4	<i>Uniqueness of names</i>	17
3.1.5	<i>Name claim dispute resolution procedure</i>	18
3.1.6	<i>Recognition, authentication and role of trademarks</i>	18
3.1.7	<i>Method to prove possession of private key</i>	18

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services
Version 1.2 of January 10, 2007

3.1.8	Authentication of organization identity	18
3.1.8.1	Class 2 (MBA/SISAC Basic Assurance Level)	18
3.1.8.2	Class 3 (MBA/SISAC Medium Assurance Level)	19
3.1.9	Certificates for affiliated individuals	19
3.1.10	Authentication of individual identity	20
3.1.10.1	Class 2 (MBA/SISAC Basic Assurance Level)	20
3.1.10.2	Class 3 (MBA/SISAC Medium Assurance Level)	21
3.1.11	Certificates for Electronic Devices	21
3.2	ROUTINE REKEY OR RENEWAL	21
3.3	REKEY AFTER REVOCATION	22
3.4	REVOCATION REQUEST	22
4	OPERATIONAL REQUIREMENTS.....	23
4.1	CERTIFICATE APPLICATION	23
4.2	CERTIFICATE ISSUANCE.....	23
4.3	CERTIFICATE ACCEPTANCE.....	23
4.4	CERTIFICATE SUSPENSION AND REVOCATION	24
4.4.1	Circumstances for revocation	24
4.4.2	Who can request revocation.....	24
4.4.3	Procedure for revocation request.....	24
4.4.4	Revocation request grace period.....	24
4.4.5	CRL issuance frequency (if applicable)	25
4.4.6	CRL checking requirements	25
4.4.7	On-line revocation / status checking availability.....	25
4.4.8	On-line revocation checking requirements	25
4.4.9	Other forms of revocation advertisements available.....	25
4.4.10	Checking requirements for other forms of revocation advertisements	26
4.4.11	Special requirements regarding key compromise	26
4.5	SECURITY AUDIT PROCEDURES	26
4.6	RECORDS ARCHIVAL	26
4.6.1	Retention Period for Audit Logs.....	28
4.7	KEY CHANGEOVER	28
4.8	COMPROMISE AND DISASTER RECOVERY	28
4.9	CA TERMINATION	29
5	PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS.....	30
5.1	PHYSICAL CONTROLS	30
5.2	PROCEDURAL CONTROLS	31
5.3	PERSONNEL CONTROLS	31
6	TECHNICAL SECURITY CONTROLS.....	33
6.1	KEY PAIR GENERATION AND INSTALLATION.....	33
6.1.1	Key pair generation.....	33
6.1.1.1	CA key pair generation.....	33
6.1.1.2	Subscriber key pair generation	33
6.1.2	Private key delivery to entity.....	33
6.1.3	Public key delivery to certificate issuer.....	34
6.1.4	Public key delivery to users.....	34
6.1.5	Key sizes.....	34
6.1.6	Public key parameters generation.....	34
6.1.7	Parameter quality checking	34
6.1.8	Hardware / software key generation.....	34
6.1.9	Key usage purposes (as per X.509 v3 key usage field).....	34
6.2	PRIVATE KEY PROTECTION	35
6.2.1	Standards for cryptographic module.....	35
6.2.2	Private key (n out of m) multi-person control	35
6.2.3	Private key escrow	35

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services
Version 1.2 of January 10, 2007

6.2.4	<i>Private key backup</i>	35
6.2.5	<i>Private key archival</i>	36
6.2.6	<i>Private key entry into cryptographic module</i>	36
6.2.7	<i>Method of activating private key</i>	36
6.2.8	<i>Method of deactivating private key</i>	36
6.2.9	<i>Method of destroying private key</i>	36
6.3	OTHER ASPECTS OF KEY PAIR MANAGEMENT	37
6.3.1	<i>Public key archival</i>	37
6.3.2	<i>Usage periods for the public and private keys</i>	37
6.4	ACTIVATION DATA	37
6.5	COMPUTER SECURITY CONTROLS	37
6.6	CA CRYPTOGRAPHIC HARDWARE LIFE CYCLE CONTROLS	38
6.7	NETWORK SECURITY CONTROLS	38
6.8	CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS	38
7	CERTIFICATES AND CRL PROFILES	40
7.1	CERTIFICATE PROFILE	40
7.1.1	<i>Version number(s)</i>	40
7.1.2	<i>Certificate extensions</i>	40
7.1.3	<i>Algorithm object identifiers</i>	42
7.1.4	<i>Name forms</i>	42
7.1.5	<i>Name constraints</i>	42
7.1.6	<i>Certificate policy Object Identifier</i>	42
7.1.7	<i>Usage of Policy Constraints extension</i>	42
7.1.8	<i>Policy qualifiers syntax and semantics</i>	42
7.1.9	<i>Processing semantics for the critical certificate policy extension</i>	42
7.2	CRL PROFILE	42
7.2.1	<i>Version number(s)</i>	42
7.2.2	<i>CRL and CRL entry extensions</i>	42
8	SPECIFIC ADMINISTRATION	44
8.1	SPECIFICATION CHANGE PROCEDURES	44
8.2	PUBLICATION AND NOTIFICATION POLICIES	44
8.3	CPS APPROVAL PROCEDURES	44
9	REFERENCES	45
10	GLOSSARY	46

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

1 Introduction

This document, the Chosen Security, Inc. Certificate Policy and Certification Practice Statement for Mortgage Industry Certificate Management Services, referred to in this document as the "Mortgage Industry CP/CPS" or shorter "CP/CPS", is a combination of Chosen Security's Certificate Policy Definitions ("CPD") and Chosen Security's Certification Practice Statement ("CPS"). The purpose of this combined CP/CPS is to document Chosen Security's policies and practices for the SISAC Accredited Certificate Management Service ("Mortgage Industry CMS"), a service designed to meet the requirements of the mortgage industry as defined in Certificate Policy Requirements Document, Version 1.4 dated April 14, 2004 ("CPRD") issued by Secure Identity Services Accreditation Corporation, a subsidiary of the Mortgage Bankers Association of America ("MBA/SISAC").

In the CPRD, Certification Authorities are referred to as Issuing Authorities. The terms are synonymous, and in this CP/CPS the term Certification Authority (CA) is used.

1.1 Overview

A Certification Practice Statement (CPS) is a statement of the practices which a Certification Authority (CA) employs in issuing certificates to a subscriber. This includes certificate application, use, and revocation or suspension of the certificate.

Certificate Policy Definitions describe the steps a CA undertakes to verify the correctness of data before a certificate is issued. The purpose of a CPD is to allow an estimation of the trustworthiness of the certificates issued by the CA.

Certificates are used with public key encryption, which is a technique where any participating entity has a key pair. One of these keys is private and must be kept secret; the other is public and is made available for retrieval from a public key directory, much like telephone numbers in a public phone book. Anything encrypted with the private key can only be decrypted with the corresponding public key (and vice versa). This can be used to implement digital signatures: The sender encrypts data using his private key, and any recipient is able to verify its integrity by using the corresponding public key available from a public key directory. The sender may also encrypt the data using the recipient's public key, ensuring that only the intended recipient is able to decrypt it using the corresponding private key.

A certificate is, in essence, a digitally signed public key. It always contains the name of the holder of the corresponding private key, who is called the subscriber. If the certificate is issued for an electronic device, for example a web-server, the subscriber is the company running the electronic device. Since anyone can create a public key with any given name, it is essential to verify that a certificate retrieved from a directory or obtained from some other source actually belongs to the subscriber named therein, because otherwise signatures might be forged and confidential data might be decrypted by unauthorized persons.

A CA acts as a trusted third party that binds certificates to the indicated entity. A certificate issued by a CA contains the subscriber's name, the name of the CA, the subscriber's public key, and is signed by the CA. Chosen Security issues certificates compliant with the requirements of the MBA/SISAC as described in this CP/CPS. Chosen Security's services are provided on the basis of a direct contract with the customer. The customer is responsible for the registration of subscribers.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

This CP/CPS describes Chosen Security's policies and practices for the Mortgage Industry CMS Service, a service designed to meet the requirements of the mortgage industry as defined in the Mortgage Bankers Association - Secure Identity Services Accreditation Corporation's (MBA/SISAC) Certificate Policy Requirements Document, Version 1.4 dated April 14, 2004 ("CPRD").

Chosen Security issues certificates in four Classes, Classes 0-3. This CP/CPS describes how two of these Classes, the Chosen Security Classes 2 and 3, correspond to two of the levels of assurance defined in the Mortgage Bankers Association CMS, Level Basic and Level Medium.

TC Class 2 certificates meet the requirements of the MBA/SISAC Basic assurance level; TC Class 3 certificates meet the requirements of the MBA/SISAC Medium assurance level.

In the future Chosen Security may expand its services to support the MBA/SISAC High assurance level.

This CP/CPS does neither constitute a declaration of self-escrow, nor does it state legally binding warranties. Any legally binding statements by Chosen Security are made in the General Terms and Conditions or in specific contracts between Chosen Security and other parties.

This CP/CPS makes extensive use of the vocabulary related to the field of digital signatures and certificates, cryptography and public key encryption, which is referenced in the Glossary (Chapter 10). The glossary also provides the definitions of some important terms not appearing elsewhere in this text that relate to the areas mentioned above.

1.2 Identification

Chosen Security, Inc. (referred to as "Chosen Security" in this CP/CPS), is the owner of TC TrustCenter GmbH of Sonninstrasse 24-28, 20097 Hamburg, Germany, an international Certification Authority and Certification Services Provider (CSP) which is the actual provider of the Mortgage Industry CMS.

This CP/CPS supports all certificates issued by Chosen Security for the Mortgage Industry CMS, which certificated are referred to as Basic and Medium assurance certificated in the CPRD.

Chosen Security has assigned an Object Identifier (OID) to each of the certificate types supported by this CP/CPS. The object identifier values used for the three classes of end-entity certificates are:

- | | |
|-----------------------------------|------------------------------|
| • Class 2, Assurance Level Basic | OID 1.2.276.0.44.1.1.6.12.1. |
| • Class 3, Assurance Level Medium | OID 1.2.276.0.44.1.1.6.12.2 |
| • Device Certificates | OID 1.2.276.0.44.1.1.6.12.3 |

1.3 Community and Applicability

This CP/CPS adheres to the structure laid out in [RFC2527], "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", © 1999 by the Internet Society, in order to facilitate comparison with other Certification Practice Statements and to ease interoperability between the certificates issued by different CAs, thereby promoting electronic commerce.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

1.3.1 Certification authorities

Chosen Security operates a Certification Authority (“CA”). It provides certification services for external third parties and issues certificates under its own certificate policies. Chosen Security provides information about other subsidiary or cooperating CAs upon request.

1.3.2 Registration authorities

A Registration Authority (RA) assists a CA by performing certificate enrollment functions. RAs confirm identities, approve or deny certificate applications, request revocation of certificates, and approve or deny renewal requests.

Chosen Security does not function as an RA in connection with providing Mortgage Industry CMS. The RA function is the responsibility of the CMS Customer which has contracted with Chosen Security to provide Mortgage Industry CMS.

1.3.3 End entities

In the context of this CP/CPS, end entity (or end user) is a synonym for Subscriber.

1.3.4 Applicability

This CP/CPS applies to all users of the Chosen Security Mortgage Industry CMS including Chosen Security, CMS Customers, Subscribers, and Relying Parties.

MBA/SISAC CPRD recommends using Basic assurance and Medium assurance certificates as follows:

Basic: This level is relevant to environments where the risks and consequences of data compromise are not considered by the Subscriber to be of major significance. This may include access to private information where the likelihood of malicious access is not high.

Medium: This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.

Certificates at High assurance level are currently not supported by Chosen Security Mortgage Industry CMS.

The determination of assurance level is made by the Subscriber only and Chosen Security makes not determination as to which level a Certificate may be appropriate for any Subscriber.

Device certificates are issued at a single assurance level. Device certificates identify a particular device within an organization and the application of that device. Examples of Device certificates include SSL Server and IPSEC VPN certificates.

1.4 Contact details

Specification administration organization

This CP/CPS is administered by Chosen Security’s Policies and Practices Board.

**Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services**

Version 1.2 of January 10, 2007

Contact person

TC TrustCenter GmbH
Certification Practice Administrator
Sonninstrasse 24-28
20097 Hamburg
Germany
Phone: +49 (0)40 808026-0
Fax: +49 (0)40 808026-126
E-Mail: pkipolicy@trustcenter.de

or

Chosen Security, Inc
Certification Practice Administrator
1000 Highland Avenue
Suite 200
Needham, MA 02494
+1 (781) 559 3312
781-559-3298

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services
Version 1.2 of January 10, 2007

2 General Provisions

2.1 Obligations

2.1.1 CA obligations

The primary purpose of any Certification Authority is to provide Certificate management services (generation, operational use, Suspension, Revocation and Expiry) for customers within their respective policy domain(s).

The CA uses its own key pairs. The private keys of the CA certificates are used to sign certificates to Subscribers. The Subscriber's key length is determined by this CP/CPS and by the CPRD.

The CA's keys are generated on a Hardware Security Module (HSM) in a physically secure facility at Chosen Security's premises in accordance with the CPRD.

The CA performs the following functions:

1. Generate its own keys
2. Operate the Certification Authority in an efficient and trustworthy manner and in accordance with this CP/CPS.
3. Establish subordinate Registration Authorities
4. On the receipt of a authenticated certificate request, issue certificates that meet the X.509 certificate standard and the requirements of the request, ensuring that the certificates are free from data entry errors and factually correct based on the information known to the CA at the time of issue
5. Revoke certificates on receipt of authenticated revocation requests, or in compliance with § 3.4 or § 4.4 of this CP/CPS
6. Post Revocation information to its OCSP responders or issue CRLs
7. Promptly notify the owner of the certificate about the revocation
8. Conduct regular internal security audits (at least annually).

In addition, the CA may reserve the right to investigate compromise and suspected compromises of private keys, non-compliance or suspected non-compliance with the stipulations of this CP/CPS in order to protect the integrity of the Mortgage Industry CMS Service, and take actions it deems appropriate based on its findings.

Investigation may include, but is not limited to:

1. Interviews with operational staff of RAs
2. A review of applicable system logs, operational records and other related files or documents, including e-mails
3. An audit of operational procedures
4. An audit of security controls, procedures and measures
5. Request for information.

These rights and obligations may be addressed in greater detail in the contractual agreements.

2.1.2 RA obligations

Chosen Security does not carry out the RA function as part of the Mortgage Industry CMS. The RA function is carried out by the CMS Customer, and the respective rights and obliga-

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

tions of the parties are set forth in the contract between Chosen Security and the CMS Customer.

An RA must not use the private RA keys for any other purpose than those associated with its RA function without the express permission of Chosen Security. The RA must comply with the provisions in this CP/CPS; this includes, but is not limited to: ensuring that the requirements specified in § 4 are met, and that the controls defined in § 5 and § 6 are provided; keeping subscriber information confidential according to § 2.8; and performing the authentication procedure as defined in § 3.

Any RA must have properly qualified and trustworthy employees that are authorized to perform the RA duties. The workstation used for submitting registration information to Chosen Security must not be publicly accessible, and the communication via insecure channels must be properly protected.

Chosen Security reserves the right to prohibit performing RA services on behalf of Chosen Security, if an RA does not conform to the provisions set forth by Chosen Security.

2.1.3 Subscriber obligations

The Subscriber obligations are described in the Subscriber Agreement.

The Subscriber Agreement requires that Certificate Subscribers provide complete and accurate information on their certificate application and agree to the subscriber agreement.

Subscribers must use their keys and certificates in a manner and for a purpose consistent with the requirements of this CP/CPS and the CPRD, especially the protection of private keys.

The key length of a Subscriber's keys is specified in this CP/CPS.

If a Subscriber discovers or has reason to believe there has been a compromise of the private key or the associated password/PIN, or the information within the certificate is incorrect or has changed, the subscriber must promptly

- Notify either Chosen Security or the RA which approved the certificate application and request revocation of the certificate in accordance with § 3.4 and § 4.4.3
- and
- Notify any person that may reasonably be expected by the subscriber to rely on the subscriber's certificate.

Subscribers have to cease use of their private key at the end of the key usage period.

2.1.4 Relying Party obligations

Prior to relying on a Certificate issued by Chosen Security pursuant to this CP/CPS, a Relying Party must review and agree to the Relying Party obligations set forth in this CP/CPS and the Relying Party Agreement. Different applications require different levels of security, and the Relying Party is solely responsible for making the decision to rely on digitally signed data verifiable by the respective Certificate in the given application context, and for checking that the Certificate is neither invalid nor revoked.

2.1.5 Repository obligations

Chosen Security provides a publicly accessible Repository containing information about certificates that have been issued, as well as other certificate related information (e.g. certificate revocation status information).

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

In addition the Repository stores a current copy, or a link to a current copy, of the CP/CPS, and other information relevant to certificates.

Chosen Security will update the repository within a reasonable amount of time to reflect new information concerning the validity and reliability of the certificates issued.

2.1.6 Certificate Revocation and Renewal

Certificate revocation is described in § 4.4.

2.2 Liability

2.2.1 Limited Warranty/Disclaimer

Chosen Security provides the following limited warranty at the time of Certificate issuance: (i) it issued the Certificate substantially in compliance with this CP/CPS; and (ii) the information contained within the Certificate accurately reflects the information provided to Chosen Security by the CMS Customer in all material respects

EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, CHOSEN SECURITY EXPRESSLY DISCLAIMS AND MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, WITH RESPECT TO THIS CP/CPS OR ANY CERTIFICATE ISSUED HEREUNDER, INCLUDING WITHOUT LIMITATION, ALL WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OR USE OF A CERTIFICATE OR ANY SERVICE (INCLUDING, WITHOUT LIMITATION, ANY SUPPORT SERVICES) PROVIDED BY CHOSEN SECURITY AS DESCRIBED HEREIN, AND ALL WARRANTIES, REPRESENTATIONS, CONDITIONS, UNDERTAKINGS, TERMS AND OBLIGATIONS IMPLIED BY STATUTE OR COMMON LAW, TRADE USAGE, COURSE OF DEALING OR OTHERWISE ARE HEREBY EXCLUDED TO THE FULLEST EXTENT PERMITTED BY LAW. EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, CHOSEN SECURITY FURTHER DISCLAIMS AND MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, TO ANY APPLICANT, SUBSCRIBER OR ANY RELYING PARTY THAT (A) THE SUBSCRIBER TO WHICH IT HAS ISSUED A CERTIFICATE IS IN THE FACT THE PERSON, ENTITY OR ORGANIZATION IT CLAIMS TO HAVE BEEN (B) A SUBSCRIBER IS IN FACT THE PERSON, ENTITY OR ORGANIZATION LISTED IN THE CERTIFICATE, OR (C) THAT THE INFORMATION CONTAINED IN THE CERTIFICATES OR IN ANY CERTIFICATE STATUS MECHANISM COMPILED, PUBLISHED OR OTHERWISE DISSEMINATED BY CHOSEN SECURITY, OR THE RESULTS OF ANY CRYPTOGRAPHIC METHOD IMPLEMENTED IN CONNECTION WITH THE CERTIFICATES IS ACCURATE, AUTHENTIC, COMPLETE OR RELIABLE.

IT IS AGREED AND ACKNOWLEDGED THAT APPLICANTS ARE LIABLE FOR ANY MISREPRESENTATIONS MADE TO CHOSEN SECURITY AND RELIED UPON BY A RELYING PARTY. CHOSEN SECURITY DOES NOT WARRANT OR GUARANTEE UNDER ANY CIRCUMSTANCES THE "NON-REPUDIATION" BY A SUBSCRIBER AND/OR RELYING PARTY OF ANY TRANSACTION ENTERED INTO BY THE SUBSCRIBER AND/OR RELYING PARTY INVOLVING THE USE OF OR RELIANCE UPON A CERTIFICATE.

IT IS UNDERSTOOD AND AGREED UPON BY SUBSCRIBERS AND RELYING PARTIES THAT IN USING AND/OR RELYING UPON A CERTIFICATE THEY ARE SOLELY RESPONSIBLE FOR THEIR RELIANCE UPON THAT CERTIFICATE AND THAT SUCH

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

PARTIES MUST CONSIDER THE FACTS, CIRCUMSTANCES AND CONTEXT SURROUNDING THE TRANSACTION IN WHICH THE CERTIFICATE IS USED IN DETERMINING SUCH RELIANCE.

THE SUBSCRIBERS AND RELYING PARTIES AGREE AND ACKNOWLEDGE THAT CERTIFICATES HAVE A LIMITED OPERATIONAL PERIOD AND MAY BE REVOKED AT ANY TIME. SUBSCRIBERS AND RELYING PARTIES ARE UNDER AN OBLIGATION TO VERIFY WHETHER A CERTIFICATE IS EXPIRED OR HAS BEEN REVOKED. CHOSEN SECURITY HEREBY DISCLAIMS ANY AND ALL LIABILITY TO SUBSCRIBERS AND RELYING PARTIES WHO DO NOT FOLLOW SUCH PROCEDURES.

Chosen Security provides no warranties with respect to another party's software, hardware or telecommunications or networking equipment utilized in connection with the use, issuance, revocation or management of Certificates or providing other services (including, without limitation, any support services) with respect to this CP/CPS. Subscribers and Relying Parties agree and acknowledge that Chosen Security is not responsible or liable for any misrepresentations or incomplete representations of Certificates or any information contained therein caused by another party's application software or graphical user interfaces. The cryptographic key-generation technology used by CMS Customers, Subscribers and Relying Parties in conjunction with the Certificates may or may not be subject to the intellectual property rights of third parties. It is the responsibility of Subscribers and Relying Parties to ensure that they are using technology that is properly licensed or to otherwise obtain the right to use such technology.

2.2.2 Limitation on Liability

EXCEPT TO THE EXTENT CAUSED BY CHOSEN SECURITY'S WILLFUL MISCONDUCT, IN NO EVENT SHALL THE CUMULATIVE LIABILITY OF CHOSEN SECURITY TO A CMS CUSTOMER, SUBSCRIBER AND/OR ANY RELYING PARTY FOR ALL CLAIMS RELATED TO THE INSTALLATION OF, USE OF OR RELIANCE UPON A CERTIFICATE OR FOR THE SERVICES PROVIDED HEREUNDER INCLUDING WITHOUT LIMITATION ANY CAUSE OF ACTION SOUNDING IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR IN ANY OTHER WAY EXCEED (A) FIVE THOUSAND DOLLARS (\$5,000.00) IN THE CASE OF BASIC ASSURANCE LEVEL CERTIFICATES OR (B) ONE HUNDRED THOUSAND U.S. DOLLARS (\$100,000.00) IN THE CASE OF MEDIUM ASSURANCE LEVEL CERTIFICATES.

CHOSEN SECURITY SHALL NOT BE LIABLE IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR IN ANY OTHER WAY (EVEN IF CHOSEN SECURITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) FOR:

(I) ANY ECONOMIC LOSS (INCLUDING, WITHOUT LIMITATION, LOSS OF REVENUES, PROFITS, CONTRACTS, BUSINESS OR ANTICIPATED SAVINGS);

(II) TO THE EXTENT ALLOWED BY APPLICABLE LAW, ANY LOSS OR DAMAGE RESULTING FROM DEATH OR INJURY OF SUBSCRIBER AND/OR ANY RELYING PARTY OR ANYONE ELSE;

(III) ANY LOSS OF GOODWILL OR REPUTATION; OR

(IV) ANY OTHER INDIRECT, CONSEQUENTIAL, INCIDENTAL, MULTIPLE, SPECIAL, PUNITIVE, EXEMPLARY DAMAGES

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

IN ANY CASE WHETHER OR NOT SUCH LOSSES OR DAMAGES WERE WITHIN THE CONTEMPLATION OF THE PARTIES AT THE TIME OF THE APPLICATION FOR, INSTALLATION OF, USE OF OR RELIANCE ON THE CERTIFICATE, OR AROSE OUT OF ANY OTHER MATTER OR SERVICES (INCLUDING, WITHOUT LIMITATION, ANY SUPPORT SERVICES) UNDER THIS CP/CPS OR WITH REGARD TO THE USE OF OR RELIANCE ON THE CERTIFICATE.

BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, THE ABOVE EXCLUSIONS OF INCIDENTAL AND CONSEQUENTIAL DAMAGES MAY NOT APPLY TO A SUBSCRIBER AND/OR A RELYING PARTY BUT SHALL BE GIVEN EFFECT TO THE FULL EXTENT PERMITTED BY LAW.

THE FOREGOING LIMITATIONS OF LIABILITY SHALL APPLY ON A CERTIFICATE-BY-CERTIFICATE BASIS, REGARDLESS OF THE NUMBER OF TRANSACTIONS OR CLAIMS RELATED TO EACH CERTIFICATE, AND SHALL BE APPORTIONED FIRST TO THE EARLIER CLAIMS TO ACHIEVE FINAL RESOLUTION.

In no event will Chosen Security be liable for any damages to CMS Customers, Subscribers, Relying Parties or any other party arising out of or related to the use or misuse of, or reliance on any Certificate issued under this CP/CPS that: (i) has expired or been revoked; (ii) has been used for any purpose other than as set forth in the CP/CPS; (iii) has been tampered with; (iv) with respect to which the Key Pair underlying such Certificate or the cryptography algorithm used to generate such Certificate's Key Pair, has been Compromised by the action of any party other than Chosen Security (including without limitation the Subscriber or Relying Party); or (v) is the subject of misrepresentations or other misleading acts or omissions of any other party, including but not limited to Subscribers and Relying Parties. In no event shall Chosen Security be liable to the Subscriber, Relying Party or other party for damages arising out of any claim that a Certificate infringes any patent, trademark, copyright, trade secret or other intellectual property right of any party.

2.3 Financial Responsibility

2.3.1 Insurance

Chosen Security maintains and will continue to maintain Errors and Omissions insurance coverage in an amount of not less than five million dollars (\$5,000,000.00) relating to its provision of Mortgage Industry CMS..

2.3.2 Indemnification by Relying Parties and Subscribers

All Relying Party Agreements and Subscriber Agreements will provide, among other things, for the indemnification of Chosen Security and its CMS Customer for the violation by the Relying Party of Subscriber of any of their respective obligations set forth in such agreements of this CP/CPS.

2.3.3 Fiduciary relationships

Any fiduciary relationship between RA, CA, Subscriber or Relying Party is specifically disclaimed by Chosen Security. Chosen Security does not represent, or act as agent, fiduciary, or trustee of any CMS Customer, Subscriber or Relying Party.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

2.4 Interpretation and Enforcement

2.4.1 Governing law

The laws of the State of New York shall govern the enforceability, construction, interpretation, and validity of this CP/CPS.

2.4.2 Severability, survival, merger, notice

2.4.2.1 Severability

If parts of any of the provisions in this CP/CPS are inoperative or void, this will not affect the validity of the remaining provisions.

2.4.2.2 Survival

Despite the fact that this CP/CPS may eventually no longer be in effect, the following obligations and limitations of the CP/CPS shall survive: § 2.1 (Obligations), § 2.2 (Liability), § 2.4 (Interpretation and Enforcement) and § 2.8 (Confidentiality).

2.4.2.3 Merger

Any modification of the provisions of this CP/CPS directly affecting Chosen Security's rights and obligations must be published as a digitally signed message or document, except as provided elsewhere in this CP/CPS.

2.4.2.4 Notice

Whenever any party wishes to or has to notify any other party with respect to this CP/CPS, such a notice shall be given by digitally signed e-mail or in writing.

The former must be sent to

pkipolicy@trustcenter.de,

the latter must be delivered either by certified mail (including return receipt request), or by a courier service confirming the delivery in writing, and it must be addressed to:

TC TrustCenter GmbH
CA Administration
Sonninstrasse 24-28
20097 Hamburg
Germany

or

Chosen Security, Inc
CA Administration
1000 Highland Avenue
Suite 200
Needham, MA 02494

Electronic e-mail must be confirmed by the recipient within one week, by digitally signed e-mail. If the sender does not receive a confirmation within the specified time period, the notice must be re-sent in writing as described above.

2.4.3 Dispute resolution procedures

Dispute resolution procedures relating to disputes between Chosen Security and CMS Customers are set for the in the agreements between the parties. Dispute resolution procedures relating to disputes between Chosen Security and Subscribers or Relying Parties are set forth the in the Subscriber Agreements and Relying Party Agreements.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

2.5 Fees

Chosen Security may charge CMS Customers and/or Subscribers for the issuance, management, and renewal of certificates.

Chosen Security does not charge a fee for making a certificate available in a Repository or otherwise making certificates available to Relying Parties.

Chosen Security does not charge a fee for publishing the CRLs required by § 4.4.5.

Chosen Security may, however, charge a fee for providing customized repositories, CRLs, OCSP services, or other value-added revocation and status information services.

Notice of any changes in fees by Chosen Security to an end entity will be brought to the attention of such entity and MBA/SISAC no less than thirty days in advance. Should fees be increased every Subscriber has the right to terminate its agreement with Chosen Security without penalty.

2.6 Publication and Repository

2.6.1 Publication of CA information

Chosen Security will publish this CP/CPS in the repository at <http://www.trustcenter.de/repository>. The directory of all certificates issued by Chosen Security and Chosen Security's issuer (root) certificates, which may also be used for on-line certificate status inquiries, is accessible from the repository as well. The Certificate Revocation List is available upon request by e-mail and from <http://www.trustcenter.de/crl>. Chosen Security may also offer an OCSP service for certificate status requests.

2.6.2 Frequency of publication

This CP/CPS and any subsequent changes shall be made publicly available within one week of approval.

CRLs are updated at least weekly. Details can be found in § 4.4.5. The certificate database is updated every time a certificate is issued. Any other information listed in § 2.6.1 is updated every time it is modified.

2.6.3 Access controls

Only authorized personnel is able to publish or modify any information referred to in § 2.6.1.

2.6.4 Repositories

For the location of the certificate repository the CP/CPS please refer to § 2.6.1. The Chosen Security support center is available at the following URL: <http://www.trustcenter.de/support>.

2.7 Compliance audit

Chosen Security is subject to regular external audits. These include audits pursuant to the German Digital Signature Act and Chosen Security acting as a CSP for Identrust Level One Participants. In the future these audits will be extended to compliance with the WebTrust™ program for Certification Authorities.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

All of these audits require demonstration of a maximum level of security and conformity to documented policies and practices. The respective provisions supplement one another and serve to enhance the overall security controls, which are audited regularly by an independent third party.

Auditing of MBA/SISAC requirements not covered by the above mentioned audits will be performed by an MBA/SISAC accredited auditor to ensure that all MBA/SISAC requirements are met.

Topics covered by these audits include checks of proper implementation of Chosen Security's certificate policies and extensive checks on key management policies, security controls, operations policy and comprehensive checks on certificate profiles.

The results of these compliance audits are documented and archived. They may be released at the discretion of Chosen Security's management.

2.8 Confidentiality

Chosen Security keeps information confidential as it is described in the contract between Chosen Security and the customer.

2.9 Intellectual Property Rights

Key pairs corresponding to certificates of Chosen Security's CAs are the property of Chosen Security.

Key pairs corresponding to certificates of subscribers are the property of the subscribers that are named in these certificates.

This CP/CPS is the intellectual property of Chosen Security.

3 Identification and Authentication

3.1 Initial Registration

In order to obtain a Certificate, any Subscriber must apply for a certificate, and identify and authenticate himself to Chosen Security's CMS Customer. This section covers these topics in a general fashion. Further details can also be found in this document.

Within the context of classification into certificate classes a distinction is made between individuals and organizations. Certificates for individuals who do not provide information about their affiliation to an organization do not contain statements about an organization which the certificate holder belongs to. Contrary to the foregoing, organizational certificates always contain a statement regarding an organization. These certificates may either be attributed to an organization (such as device certificates which cannot be attributed to natural persons) or they may be attributed to a member of an organization, such as an employee of a company, for example. Information about an organization must be entered into all organizational certificates

3.1.1 Types of names

All names specified in X.509 certificates must be expressed as X.509 Distinguished Names (DNs).

This CP/CPS provides examples for proper certificate names.

3.1.2 Need for names to be meaningful

If the subscriber's key pair is generated by Chosen Security or one of its cooperating CAs (see § 6.1), Chosen Security will determine the subscriber's DN to make it compliant with common standards, practices and other regulations.

If the subscriber generates its own key pair, the name should be chosen to be meaningful to any relying party, i. e. the name form should have commonly understood semantics (first and last name, company's name, Internet e-mail address) for the relying party to determine identity of the person and / or organization. Chosen Security will check subscriber DN's for compliance with common standards, practices, and other regulations, and may, at its own discretion, alter a subscriber DN accordingly.

Please check this CP/CPS for examples.

3.1.3 Rules for interpreting various name forms

Any X.509 certificate issued for private use will have empty Organization and Organizational Unit fields. If one (or both) of these fields are present, the certificate is either intended for commercial use or sponsored by that organization.

3.1.4 Uniqueness of names

Any subscriber DN in a certificate issued by Chosen Security must uniquely identify a single entity among all of Chosen Security's subscribers. If necessary, Chosen Security may append additional numbers or letters to an actual name in order to ensure the name's uniqueness.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

The same entity may have different certificates all bearing the same subject DN, but no two separate entities may share a common DN (and be issued by the same CA). In any case, there must not be two certificates having the same issuer DN and serial number.

3.1.5 Name claim dispute resolution procedure

Chosen Security is not responsible for resolving name claim disputes among subscribers. Chosen Security may add, at its own discretion, additional information to a name in order to make it unique among the names of certificates issued by Chosen Security.

3.1.6 Recognition, authentication and role of trademarks

Chosen Security will honor trademark claims that are documented by a subscriber.

3.1.7 Method to prove possession of private key

In order to prove a subscriber's possession of the private key corresponding to the public key contained in a certificate application, any certificate request submitted as part of a certificate application must be self-signed.

3.1.8 Authentication of organization identity

The following sections contain explanations about the verification procedures for organizations. All explanations only refer to data contained in certificates.

In addition to the verifications confirming the certificate's content Chosen Security will perform additional checks. These checks are to prove that the organization has authorized the certificate application, and that the person submitting the certificate application on behalf of the organization is authorized to do so.

This proof (called the Application Confirmation) must be signed by an authorized entity in the organization and can be sent to Chosen Security or the relevant RA by mail, e-mail, or by fax. Alternatively Chosen Security may verify the authorization to apply for a certificate by phone.

3.1.8.1 Class 2 (MBA/SISAC Basic Assurance Level)

Statements made in Class 2 certificates about organizations are verified in the following way:

- Name and registered office of an organization are verified. This verification may be carried out by a presentation of a copy of a document, which proves the existence of the organization (current extract of a competent official register in which the organization is listed or a comparable document).

Extracts being not older than 9 months are accepted as up to date.

For extracts, which have been issued between 9 and 36 months ago, an additional confirmation must be presented. This confirmation must state that the name and the legal form of the organization are still valid. If Chosen Security is already in possession of a copy of an extract of an official register it need not be sent again.

The confirmation must be presented on a paper with the official letterhead of the organization. It must be signed by an authorized person.

The confirmation may be sent by fax or e-mail. An e-mail must be signed with a certificate which fulfils at least the requirements of a TC Class 2 certificate.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

Chosen Security does not accept register extracts which are older than 36 months

The existence and correct denomination of governmental or administrative authorities must be confirmed by a competent authority (e.g. a superior authority) with official letter-head, stamped with an official stamp or seal, and signed by an authorized officer.

If an applicant requires more than one certificate but does not want them to be issued at the same time, Chosen Security may perform a pre-vetting at the time of registration or later. The actual application for the certificate is then sent later, but the results of the vetting are already present. When a certificate is issued the pre-vetting must not be more than twelve months ago.

- The correctness of an e-mail address of an organization or a member of an organization (if such is stated in the certificate) may be confirmed by a responsible person of the organization.
- Additional data in the certificate are verified as much as possible. For server certificates it is checked if the domain name in the certificate is registered to the organization applying for the certificate. In contrast to that, an automatic verification of the existence on an organizational unit (which can be stated in the OU field of the certificate) is usually not possible.

A domain registration may be checked in advance. When the certificate is issued the domain check must not be more than twelve months old.

A Team Certificate may be used by a group of persons (e.g. a department of an organization); nevertheless it is formally assigned to one person (as required by § 3.1.4), who is then responsible for the proper use of the certificate (e.g. head of department). This person must be identified in compliance with the rules for Class 2 individual certificates (or higher) of these CP/CPS.

Function Certificates are certificates, which are selected for a special purpose (e.g. automatic signature of outgoing mail). Usually they are bound to a fixed computer or application. The computer or application can use the certificate and automatically produce a multitude of signatures. Formally such a certificate is assigned to a person who is responsible for the proper use of the certificate, and this person must be identified in compliance with the rules for Class 2 individual certificates (or higher) of these CP/CPS.

All vetting may also be carried out utilizing data provided by reputable third party vendors of business information.

3.1.8.2 Class 3 (MBA/SISAC Medium Assurance Level)

In contrast to Class 2 all documents presented must be original or notarized.

Apart from that the existence and correct denomination of organizations is verified in the same manner as with Class 2 certificates.

All vetting may also be carried out utilizing data provided by trustworthy third parties.

The responsible person for a Team or Function Certificate must be identified in compliance with the rules for class 3 individual certificates.

3.1.9 Certificates for affiliated individuals

The affiliation of a person to an organization, where applicable also the affiliation to a department of the organization, must be confirmed by an authorized member of that organization. This confirmation must have a handwritten signature and a stamp of the organization

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

(for governmental agencies an official seal is needed) or it must be digitally signed. The certificate used for the digital signature must be compliant with the requirements of a Medium assurance level certificate of the MBA CMS.

3.1.10 Authentication of individual identity

The authentication of an individual entity depends upon the different certificate classes Chosen Security defines for issuing certificates.

Chosen Security and/or associated RAs shall ensure that the applicant's identity information is verified in accordance with the guidelines established by this CP/CPS.

Chosen Security and/or associated RAs shall record the information set forth below for issuance of each certificate:

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the applicant as required;
- If in-person identity proofing is done, a unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The date of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication.

3.1.10.1 Class 2 (MBA/SISAC Basic Assurance Level)

The applicant's identity may be established by in-person proofing before a Registration Authority or Trusted Agent; or remotely verifying information through record checks at trusted third party databases as credit bureaus or similar databases.

It has to be confirmed that: name, date of birth, address, and other personal information in the records are consistent with the application and sufficient to identify a unique individual.

Statements about a natural person's name and address are verified as follows:

- a) If electronic verification is chosen the applicant must send a copy of an official photo-ID. Data from this photo-ID will be confirmed by verifying consistency with an accredited third party regarding the correctness and the completeness of data;
- or
- b) If in-person proofing is chosen the applicant has to present an official, state-issued photo ID document with signature.

An entity certified by a State or Federal Entity as being authorized to confirm identities may perform in-person authentication on behalf of the RA. The certified entity forwards the information collected from the applicant directly to the RA in a secure manner. Packages secured in a tamper-evident manner by the certified entity satisfy this requirement; other secure methods are also acceptable. Such authentication does not relieve the RA of its responsibility to verify the presented data.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

3.1.10.2 Class 3 (MBA/SISAC Medium Assurance Level)

The applicant's identity can be established by in-person proofing before a Registration Authority, Trusted Agent, or an entity certified by a State or Federal Entity as being authorized to confirm identities.

It has to be confirmed that name, date of birth, address, and other personal information match the presented ID document(s).

The applicant has to present either

- A Federal Government-issued Picture ID
- or
- Two Non-Federal Government IDs, one of which must be a photo ID.

3.1.11 Certificates for Electronic Devices

Device certificates are issued at a single assurance level. Device certificates identify a particular device within an organization and the application of that device. Examples of Device certificates include SSL Server and IPSEC VPN certificates.

Because an electronic device is unable to perform face-to-face registration it may be represented by a trusted person (sponsor). The sponsor must present information sufficient for registration, for both himself/herself and the electronic device.

Device authentication includes verification (in accordance with section 3.1.9) of affiliation of the sponsor and his/her authorization to request a device certificate.

The sponsor is responsible for providing the following information:

- Equipment identification (serial number) or service name (e.g. DNS name)
- Equipment Public Key
- Equipment IP Address
- Equipment application (e.g. SSL, IPSEC)
- Contact information to enable the RA to communicate with the trusted person.

For all Levels: If a certificate contains an e-mail address, its correctness is verified by sending a random number to that e-mail address. The applicant has to respond with that number. Alternatively, for members of organizations a responsible person in that organization may confirm the correctness of the e-mail address.

3.2 Routine Rekey or Renewal

Rekey means changing the public key for an existing certificate by issuing a new certificate with a *different* (usually new) public key. The certificate name stays the same. It is different from renewal, which means issuing a new certificate, with an extended validity period, for the *same* public key. (See [RFC2828].)

The general procedure for rekey and renewal is as follows:

The subscriber must submit an authenticated renewal or rekey request (i. e., using the private key that corresponds to the certificate that should be renewed or rekeyed). The subscriber's certificate request includes at least the subscriber's distinguished name, the serial number of the certificate (or other information that identifies the certificate), and the re-

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

requested validity period. Chosen Security processes the request data to verify the identity of the requesting entity and identify the certificate to be renewed or rekeyed.

3.3 Rekey after Revocation

After a certificate has been revoked, the subscriber must generate a new key pair and reapply to Chosen Security for a (new) certificate in accordance with § 3.1, since the revoked key pair is ineligible to sign and authenticate a rekey request (see § 3.2) Renewal after revocation is not allowed.

3.4 Revocation Request

There are several ways to submit a revocation request:

1. If the subscriber is still in possession of his private key, he/she has the option of submitting an authenticated revocation request to Chosen Security.
2. If the private key has been lost or is inaccessible for any reason, the subscriber may call Chosen Security or the RA and authenticate himself by naming the revocation password chosen when submitting the initial certificate application.
3. The subscriber or an authorized third party (e.g. the organization the subscriber is affiliated to) may request a certificate to be revoked by writing a letter to Chosen Security or the RA stating this request. Authentication is provided by the subscriber's signature.

Chosen Security confirms the request for revocation, by e-mail, within reasonable amount of time, no later than twenty-four hours after receiving the request.

4 Operational Requirements

4.1 Certificate Application

A subscriber submits a certificate application to Chosen Security and follows the procedures described in Chosen Security's CP/CPS for the MBA CMS (this document):

- complete a certificate application and provide the required information
- generate a key pair in accordance with § 6.1,
- deliver the public key to Chosen Security in accordance with § 6.1.3,
- demonstrate pursuant to CP/CPS § 3.1.7 possession of the private key corresponding to the public key delivered to Chosen Security
- manifest assent to the relevant subscriber agreement.

Certificate applications are submitted to Chosen Security for processing, the result being either approval or denial.

4.2 Certificate Issuance

Chosen Security verifies, as set forth in § 3.1.7, that the applicant is in possession of the private key and that the certificate request has the proper contents, for example, that the common name field states the full server domain name in the case of server certificate requests. Chosen Security will verify the data contained in the request according to the Chosen Security CP/CPS for the MBA CMS. Chosen Security will either issue the subscriber's certificate upon successful completion of this process and notify the subscriber, or inform the subscriber of any problems or inconsistencies.

The certificate will be valid for no more than five years from the date of issuance, with a default validity period of one year. Once it has expired, the subscriber may either renew his certificate if the maximum validity period has not yet been reached, or must reapply for a new certificate otherwise.

Chosen Security generates certificates using the appropriate certificate format, and sets validity periods and extension fields in accordance with relevant standards, such as X.509. For certificate renewals, Chosen Security generates and signs a new instance of the certificate, differing from the previous certificate only by the validity period.

4.3 Certificate Acceptance

After a certificate has been issued, Chosen Security notifies the subscriber that the certificate is available and notifies the subscriber of the means for obtaining the certificate.

Certificates are made available to subscribers, either by allowing them to download them from a web site or via a message sent to the subscriber containing the certificate. For example, Chosen Security may send the subscriber an URL, where the subscriber can obtain the certificate. The certificate may also be sent to the subscriber in an e-mail message. Downloading a certificate or installing a certificate from a message attaching it constitutes the subscriber's reception of the certificate.

Usage of the private key by the subscriber, corresponding to a certificate issued by Chosen Security, is deemed to be acceptance of the certificate. It is then usable in any application

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

requiring the use of a digital certificate of that type and available from the certificate repository for verification.

By accepting a certificate, the subscriber warrants that all of the information provided by the subscriber (and by its organization, where applicable) and included in the certificate, and all representations made by the subscriber (and by its organization, where applicable) as part of the application and identification process, are true and not misleading.

4.4 Certificate Suspension and Revocation

A certificate can either be suspended or revoked. If it is not certain whether the corresponding private key has been lost or compromised, the subscriber must suspend the certificate until matters have been clarified. If the private key has been compromised or lost for sure, or if subscriber data represented in the certificate has changed substantially, the certificate must be revoked and the subscriber must reapply.

If the certificate is revoked, it becomes invalid as soon as Chosen Security has processed the revocation request. The certificate's serial number and time of revocation will be included in the Certificate Revocation List (CRL), and subsequent status inquiries to the certificate repository will result in a response citing the certificate as invalid.

If the certificate is suspended, it will be placed on the CRL, and any status inquiries to the certificate repository while the suspension is in effect will result in a response citing the certificate as invalid.

Certificate suspension may not be supported for all (or any) certificate class(es).

4.4.1 Circumstances for revocation

A certificate is revoked in case:

1. The subscriber or his agent has submitted a revocation request as described in § 3.4;
2. Chosen Security has learned about false information having been supplied in the certificate application that invalidates the certificate.

4.4.2 Who can request revocation

Only the subscriber can request revocation, except as noted in § 4.4.1, 2.: Any entity or third party that confirmed any information contained in a certification should inform Chosen Security about the fact that this information is not or no longer correct, and request revocation in accordance with § 4.4.1, 2.

If a certificate states that its holder may act on behalf of a third party, this party may also request invalidation of the certificate.

4.4.3 Procedure for revocation request

The procedure for revocation is described in § 3.4.

4.4.4 Revocation request grace period

Chosen Security processes the revocation request, upon confirming that it originated from the subscriber, as promptly and efficiently as possible. The time needed to revoke the certificate does not exceed twenty-four hours for Class 2 certificates; it does not exceed twelve hours for Class 3 certificates.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

4.4.5 CRL issuance frequency (if applicable)

Certificate status information is made available to all relevant entities through Certificate Revocation Lists (CRLs) which are available from Chosen Security's repository. CRLs are also available upon request by e-mail. Each CRL is digitally signed so that entities can validate the integrity of the CRL and the date of issuance, and it includes a monotonically increasing sequence number.

CRLs are issued at least once a week, but will in general be updated up to several times a day, even if no changes have occurred since the last issuance. At a minimum, a CRL entry identifying a revoked certificate remains on the CRL until the end of the certificate's validity period. A certificate is also put on the CRL during its suspension period.

Whenever Chosen Security determines that a Class 2 (Basic) or Class 3 (Medium) certificate from the MBA PKI is to be revoked, Chosen Security will issue and publish a new CRL with the newly revoked certificate within at most 12 hours.

CRLs are available from the following URL:

<http://www.trustcenter.de/crl>

4.4.6 CRL checking requirements

It is the responsibility of the relying party to either obtain the latest CRL and check the revocation status, or to check the revocation status on-line.

In order to check a CRL's signature, a relying party must be in possession of, or obtain, the appropriate CRL certificate. This certificate may differ from the certificate of the issuer(s) of any certificate on the CRL, and if so, it is available from Chosen Security's Web Site or upon request by e-mail.

4.4.7 On-line revocation / status checking availability

The certificate status can be checked on-line from the certificate repository. Any changes committed to the repository are immediately available to any subscriber and / or relying party.

Please see Chosen Security's Web Site for other means of checking a certificate's status (e. g. OCSP).

4.4.8 On-line revocation checking requirements

It is the responsibility of the relying party to either obtain the latest CRL and check the revocation status, or to check the revocation status on-line.

In order to check an on-line revocation status response, a relying party may need to obtain the appropriate response signing certificate. This certificate may differ from the certificate of the issuer of the certificate being checked, and if so, it is available from Chosen Security's Web Site or upon request by e-mail.

4.4.9 Other forms of revocation advertisements available

Chosen Security offers a push service to interested customers. Any time a certificate is revoked, Chosen Security will notify these customers. Details are available upon request from Chosen Security.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

4.4.10 Checking requirements for other forms of revocation advertisements

No stipulation.

4.4.11 Special requirements regarding key compromise

Depending on whether the subscriber suspects or knows for sure that his private key has been compromised, he is required to request suspension or revocation, respectively, as soon as possible. A subscriber is not relieved from his obligations as a subscriber until he has been notified by Chosen Security of the revocation of the certificate.

4.5 Security Audit Procedures

Chosen Security keeps audit trails and system log files that document actions taken as part of Chosen Security's public certification services. These include, but are not limited to: issuance of certificates, CRLs, time stamps; notification of key compromise; revocation of certificates; extension of certificates; establishment of trusted roles and actions of trusted personnel; changes to CA keys.

In addition, system access and use is monitored and recorded in audit logs or written down in event journals. Events in audit logs are time-stamped and digitally signed. Audit logs and event journals are reviewed regularly and archived to assist in future investigations of security-related incidents.

Chosen Security's policies and procedures on auditing, monitoring and event journaling cover the following areas:

- types of events recorded,
- frequency of processing log files,
- retention period for audit logs,
- protection of audit logs,
- audit log backup,
- audit collection system,
- notification to the event-causing subject and
- vulnerability assessment.

As part of the scheduled system back up procedures, audit trail files are backed up to WORM media. Audit trail files are archived by the system administrator on a regular (at least) weekly basis. Event journals are reviewed at least on a weekly basis by the internal auditors.

No single person may modify or even delete audit trails or system log files, and access to them is strictly restricted. These provisions are implemented using the features of a secure B1 operating system.

For further details upon internal and external audit requirements and procedures, see § 2.7.

4.6 Records Archival

Audit trails and system log files (see § 4.5) are backed up regularly on WORM (write once, read multiple) media and archived in a safe facility. Chosen Security uses internal and external archival to prevent loss of important documents and digital data. The archives are located

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

in separate (internal or external) locations and protected by access-control systems. Records are archived for at least five years. No single person is allowed to modify or even destroy archived material, and access to them is strictly restricted.

Audit data comprise the following events:

Security Audit: Any changes to the Audit parameters, e.g., audit frequency, type of event audited, any attempt to delete or modify the Audit logs, obtaining a third-party time-stamp.

Identification and Authentication: Successful and unsuccessful attempts to assume a role, the value of maximum authentication attempts is changed, the number of unsuccessful authentication attempts exceeds the maximum authentication *attempts* during user login, an Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts, an Administrator changes the type of authenticator, e.g., from password to biometrics.

Local Data Entry: All security-relevant data that is entered in the system.

Remote Data Entry: All security-relevant messages that are received by the system.

Data Export and Output: All successful and unsuccessful requests for confidential and security-relevant information.

Key Generation: Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys).

Private Key Load and Storage: The loading of Component private keys, all access to certificate subject private keys retained within the CA for key recovery purposes.

Trusted Public Key Entry, Deletion and Storage: All changes to the trusted public keys, including additions and deletions.

Secret Key Storage: The manual entry of secret keys used for authentication.

Private and Secret Key Export: The export of private and secret keys (keys used for a single session or message are excluded).

Certificate Registration: All certificate requests.

Certificate Revocation: All certificate revocation requests.

Certificate Status Change Approval: The approval or rejection of a certificate status change request.

CA Configuration: Any security-relevant changes to the configuration of the CA.

Account Administration: Roles and users are added or deleted, the access control privileges of a user account or a role are modified.

Certificate Profile Management: All changes to the certificate profile.

Revocation Profile Management: All changes to the revocation profile.

Certificate Revocation List Profile Management: All changes to the certificate revocation list profile.

Miscellaneous: Appointment of an individual to a Trusted Role, designation of personnel for multiparty control, installation of the operating system, installation of the CA, installing hardware cryptographic modules, removing hardware cryptographic modules, destruction of cryptographic modules, system startup, login attempts to CA applications, receipt of hardware/software, attempts to set passwords, attempts to modify passwords, backing up CA internal database, restoring CA internal database, file manipulation (e.g., creation, renaming,

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

moving), posting of any material to a repository, access to CA internal database, all certificate compromise notification requests, loading tokens with certificates, shipment of tokens, zeroizing tokens, re-key of the CA, configuration changes to the CA server involving:

- Hardware
- Software
- Operating System
- Patches
- Security Profiles.

Physical Access / Site Security: Personnel access to room housing CA, access to the CA server, known or suspected violations of physical security.

Anomalies: Software error conditions, software check integrity failures, receipt of improper messages, misrouted messages, network attacks (suspected or confirmed), equipment failure, electrical power outages, uninterruptible power supply (UPS) failure, obvious and significant network service or access failures, violations of policies, resetting Operating System clock.

4.6.1 Retention Period for Audit Logs

The minimum retention periods for archive data are identified below. CA and RAs must follow with their respective records retention policies in accordance with whatever laws apply to those entities.

This minimum retention period for these records is intended only to facilitate the operation of the MBA PKI and its CAs.

Certificate Class	MBA PKI Assurance Level	Minimum Retention Period
Class 2	Basic	7.5 Years
Class 3	Medium	10.5 Years
	High	20 Years
Class 2	Device	7.5 Years

Issuing certificates under the MBA PKI Assurance Level High is currently not supported by Chosen Security.

4.7 Key changeover

Upon the end of the private key's lifetime, a new CA signing key pair is generated and all subsequently issued certificates and, if applicable, CRLs are signed with the new private signing key. Changing CA keys enables Chosen Security to adjust key parameters, taking into account advances in science and / or technology. Any new CA key is available on request via e-mail or from Chosen Security's repository at <http://www.trustcenter.de/repository>.

4.8 Compromise and Disaster Recovery

Chosen Security has a business continuity plan to restore its business operations in a reasonably timely manner following interruption to, or failure of critical business processes. The

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

business continuity plan defines the period of time that is an acceptable system outage time in the event of a major natural disaster or CA private key compromise. This outage time depends on the certificate policy that pertains to the certification services related system that has failed and may range from one hour up to 72 hours.

Backups of essential business information and CA system software are performed daily. Chosen Security tests internal disaster recovery procedures regularly. Documentation concerning details of these procedures is considered confidential.

4.9 CA Termination

The CA can only be terminated by the Board of Directors of the CA. Subscribers of valid certificates (i. e., neither revoked nor expired) will be given as much advance notice as circumstances permit, and attempts to provide alternative sources of interoperation will be sought.

Chosen Security will make a reasonable effort to archive the records of the CA and transfer them to a specified custodian, and to establish an acceptable procedure for subscribers and relying parties for switching to a different provider of public certification services, in order to minimize the effects of Chosen Security ceasing to provide these services by itself.

If no alternative certificate provider continues Chosen Security's services all certificates that have not expired or have not been revoked by the respective subscribers will be revoked by Chosen Security. Subscribers will be notified of such action taken by Chosen Security.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

5 Physical, procedural, and personnel security controls

Chosen Security is committed to establishing and maintaining state of the art security controls required of CAs and RAs. This chapter provides an outline of such a security controls framework, which reflects the provisions of the Digital Signature Act, the Identrust System, the WebTrust™ Program for Certification Authorities, and the requirements for MBA/SISAC. The respective provisions supplement one another and serve to enhance the overall security controls, which are audited regularly by independent third parties. The Digital Signature Act, WebTrust™, and Identrust practices require the highest standards of security controls.

For security reasons, however, Chosen Security will not disclose any specific details about the specific measures taken. The documents describing Chosen Security's implementation of security controls are considered non-public.

Note: As of this writing, TC TrustCenter as the actual provider of the Mortgage Industry CMS has been approved as a third-party certification services provider to several Identrust Level One Participants. In addition, TC TrustCenter obtained an accreditation as a German Digital Signature Act-compliant Certification Authority, which implies a successful audit against all the requirements in this CP/CPS. Because the German Digital Signature Act is more restrictive than the European Signature Guidelines this also proves compliance with the relevant laws and standards of the European Union. An audit for WebTrust™-compliance is in preparation.

5.1 Physical Controls

Several layers of physical security controls restrict access to Chosen Security's sensitive hardware and software systems used in performing critical CA operations, which take place within a physically secure facility. These systems are physically separated from the organization's other systems so that only authorized employees of the CA can access them.

Physical access to the CA systems is strictly controlled. Only trustworthy individuals with a valid business reason are provided such access. The access control system is always functional and utilizes access cards and passwords for access. A log is maintained, listing all physical entries to restricted areas.

Private keys used for issuing certificate or signing CRLs are not vulnerable to physical penetration. These keys are kept in tamper-resistant hardware modules. Any unauthorized access to stored information, possibly resulting in loss, tampering or misuse thereof, is prevented by proper means. Regular security checks are made to ensure that all these controls function properly.

Access to any physical area where information or equipment sensitive to CA operations is located requires at least two persons authorized to access the respective locations. Entering restricted areas using the same authorization token twice (to circumvent the requirement of two *different* persons having to access the respective location) is prevented by technical means. In addition, sensitive areas are monitored by video cameras.

Any sensitive computer system with regard to certificate issuance runs a secure B1 operating system and cannot be operated through a LAN or WAN, but only from the console. The computer systems providing the directory and repository services may only be administered from the console or via a secure network protocol. Access to sensitive systems requires two persons to be present (or log on) simultaneously.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

All CA systems have industry standard power and air conditioning systems to provide a suitable operating environment. All CA systems have reasonable precautions taken to minimize the impact of water exposure. All CA systems have industry standard fire prevention and protection mechanisms in place.

Off-site backups are stored in a physically secure manner by a bonded third-party storage facility.

Any RA confirming subscriber information and forwarding this information to Chosen Security must provide a secure physical facility for storing registration records and tokens needed to access RA components. If an RA keeps confidential subscriber information, such as subscriber key information or application data and identification records, the RA's physical security controls must match those of Chosen Security.

5.2 Procedural Controls

Chosen Security's operating procedures are documented and maintained. Procedural controls ensure that no single person acting by itself will be able to circumvent the security measures taken.

Formal management responsibilities and procedures exist to control all changes to CA equipment, software, and operating procedures. Duties and areas of responsibility are segregated in order to reduce opportunities for unauthorized modification or misuse of information or services. This is achieved, for example, by defining different roles so that performing certain essential tasks requires multiple individuals to prevent a single person from being able to forge a certificate.

Development and testing facilities are separated from operational facilities. Procedures exist and are followed for reporting software malfunctions. Procedures exist and are followed to ensure that faults are reported and corrective action is taken. Users of CA systems are required to note and report observed or suspected security weaknesses in or threats to systems or services. System documentation is protected from unauthorized access.

Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

Detection and prevention controls to protect against viruses and malicious software and appropriate user awareness procedures are implemented.

A formal reporting procedure exists and is followed, together with an incident response procedure, setting out the action to be taken on receipt of an incident report. Incident management responsibilities and procedures exist and are followed to ensure a quick, effective, and orderly response to security incidents.

5.3 Personnel Controls

Chosen Security ensures that the personnel involved in issuing, managing, suspending and revoking certificates and managing related data and information is integer, trustworthy and loyal. This includes, but is not limited to, requiring a certificate issued by the police, stating that the individual in question has no criminal record whatsoever. It must have proper knowledge and experience related to CA operations and must have demonstrated security consciousness and awareness regarding its duties at Chosen Security. Periodic reviews occur to verify the continued trustworthiness of all personnel.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

Employees sign a confidentiality (nondisclosure) agreement as part of their initial terms and conditions of employment. All employees of the organization and, where relevant, third-party users, receive appropriate training in organizational policies and procedures.

A formal disciplinary process exists and is followed for employees who have violated organizational security policies and procedures. Chosen Security's policies and procedures specify the sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems.

Appropriate and timely actions are taken when an employee is terminated so that controls and security are not impaired by such an occurrence.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

6.1.1.1 CA key pair generation

Any private CA key used for issuing certificates for the MBA CMS is generated on a hardware security module (HSM) evaluated as "E4 high" according to ITSEC criteria (or equivalent), or using a FIPS 140-1 Level 3-compliant HSM, which is tested for proper operation before commencing the key generation procedure. The entire procedure is done under dual control. In addition, the key generation is witnessed and signed off by a third person not involved in the actual key generation.

At no point during the generation process does the private key leave the HSM in unencrypted form, and no unencrypted private key material leaks out.

No copy of any private key is kept permanently on magnetic media in unencrypted form, and any private key material that was temporarily stored on magnetic media is destroyed by wiping the space once occupied by the respective file(s) multiple times to erase any remaining trace. Alternatively, instead of wiping magnetic media, it may be physically destroyed.

6.1.1.2 Subscriber key pair generation

The subscriber can generate its key pair using software generating certificate requests in any format Chosen Security can process (X.509, WTLS), like Internet browsers, Web servers, security proxies etc. The key generation may happen during the certificate application, depending on what kind of certificate the subscriber wishes to apply for.

The key pair may also be generated by Chosen Security or one of its cooperating CA agencies. This may happen, for example, if the secret key is stored on a Smart card. In this case, Smart cards used will generally be able to autonomously generate the key pair and be evaluated as "E4 high" according to ITSEC criteria (or equivalent). Chosen Security then merely initiates this process and has no control over or access to private key material.

6.1.2 Private key delivery to entity

If the subscriber generates its own key pair, there is no need for private key delivery to the end user.

If Chosen Security generates the key and stores it on a hardware token (such as a Smart card), the private key (i. e., the hardware token) and the sealed letter containing the PIN(s) needed to use or enable the private key may either

- (1) be delivered to the end user, upon his request, by certified mail with return receipt or any other acceptable form of secure delivery, or
- (2) be collected by the end user at Chosen Security's office or at one of the RAs.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

6.1.3 Public key delivery to certificate issuer

If the key pair is generated by the subscriber, then the self-signed public key has to be submitted to Chosen Security during certificate application.

If Chosen Security generates the key pair on behalf of the user (see § 6.1.1.2), there is no need for public key delivery to the certificate issuer.

6.1.4 Public key delivery to users

The CA's public keys are available from the certificate repository and upon request by e-mail.

The subscriber's public key is either delivered by e-mail or by means of delivery of the physical hardware token (smart card) used for storing the subscriber's key pair. During certificate generation, the CA system checks that the end entity's certificate can be verified using the issuing CA's public key. If the subscriber has agreed to his certificate being published in Chosen Security's certificate directory, it is available for download as well.

6.1.5 Key sizes

The X.509 CA keys are at least 2048 bit in size. Subscriber's public keys must be between 512 and 4096 bit in size, with 2048 bit recommended.

Any key generated on a smart card is currently 1024 bit in size. As soon as such cards are available Chosen Security will also support smart cards with larger keys.

6.1.6 Public key parameters generation

Public key parameters for key pairs generated by software are determined by the configuration of the generating application. They may include key size, key ID, key type (e. g., Diffie-Hellman or RSA), date of creation, validity period, etc.

Public key parameters for key pairs generated by hardware are determined by the hardware's capability. They are chosen to ensure the best possible security, i. e., the optimal key size and reliable encryption / signature algorithms that are offered by the hardware are used.

All current CA keys are RSA keys and use the MD5, SHA-1, or SHA-2 hash algorithm.

6.1.7 Parameter quality checking

The online-application and / or certification mechanisms will check for properly generated certificate requests and their correct format.

6.1.8 Hardware / software key generation

Subscribers may generate their key pairs with whatever soft- or hardware is available to them. Chosen Security recommends to use the strongest type available, and tamper-proof hardware tokens (like smart cards) are to be preferred for storage of secret keys.

6.1.9 Key usage purposes (as per X.509 v3 key usage field)

Certificates issued by Chosen Security must be used according to the X.509 v3 key usage field as set by Chosen Security (see also § 7.1). Certificates may, in general, be used for any purpose, including Web server security and code signing, except as provided in this CP/CPS.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

6.2 Private Key Protection

Chosen Security keeps its private keys in a trusted computer system not connected to Chosen Security's local area network or any public network. The computer system is kept in a secure physical facility. Access to both the facility and the private keys is protected by access control mechanisms. The private keys can only be activated under dual control and are, once decrypted using the proper authorization, never written to any permanent or magnetic storage media.

6.2.1 Standards for cryptographic module

For signing X.509 keys, a cryptographic hardware module is used. This Hardware Security Module (HSM) has two modes of operation which meet either FIPS 140-1 level 2 or FIPS 140-1 level 3 criteria. Physical access to the cryptographic module is restricted by an access control system. The HSM must be activated by two persons simultaneously (dual login). The HSM which stores the private keys for issuing certificates in the MBA CMS is used in the FIPS 140-1 level 3 mode.

Also two persons are required to insert and activate the smart cards that hold the private CA keys used for issuing certificates.

An unencrypted private key cannot be extracted from the hardware module at any point.

6.2.2 Private key (n out of m) multi-person control

The private CA keys are stored encrypted in a secure physical facility operated by TC TrustCenter. In order to gain access to the private keys, at least two persons are required (see § 6.2.1). No single person has all the activation data needed for accessing any of the private CA keys.

6.2.3 Private key escrow

Chosen Security will not keep end users' private keys or any private key material, unless

- (1) key escrow is explicitly agreed upon in a contract between the subscriber and Chosen Security, outlining the liabilities and remedies between the parties, and
- (2), is not prohibited by law, certificate policies or other applicable provisions or agreements.

For recovery purposes only keys used for encryption and decryption may be escrowed. Keys for Digital Signature are never escrowed.

Using key escrow is strongly discouraged, however, since the risks generally outweigh the benefits.

If CA private signing keys are held in escrow, escrowed copies of the CA private signing keys are subject to the same or greater level of security controls as keys currently in use.

For certificates issued in compliance with the German Digital Signature Act any form of key escrow is explicitly prohibited by the German Digital Signature Act.

6.2.4 Private key backup

Chosen Security keeps backup copies of its private CA keys in encrypted form. These keys can only be activated under dual control in a physically secure site (see § 5.1).

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

Keys generated and stored on a smart card cannot be extracted from the smart card and are therefore not backed up.

Subscribers may backup their own private keys. In this case keys must be copied and stored in encrypted form and protected at the same level as the primary key.

6.2.5 Private key archival

Chosen Security uses daily, weekly, monthly, and yearly backup media (see § 6.2.4) for archival. Subscribers may archive their own private keys. The stipulations on private key backup apply.

All archived CA keys are destroyed at the end of the archive period using dual control in a physically secure site. Archived keys are never put back into production.

6.2.6 Private key entry into cryptographic module

Private keys are stored on the CA system in encrypted form. They can only be activated under dual control. Unencrypted keys are kept inside HSM during their usage only, and are never stored on the host in the clear, except where using an HSM is not possible.

6.2.7 Method of activating private key

Activating private keys requires authentication via pass phrases and / or PINs and can only be done under dual control, since the authentication secret is split into two or more shares. Where an HSM is used, activation of the private key additionally requires possession of a hardware token (smart card).

6.2.8 Method of deactivating private key

The private key is automatically deactivated after issuing certificates has been completed and the certification application exits or closes the connection to the HSM. Before it can be used again, it must be reactivated.

6.2.9 Method of destroying private key

The destruction of any private CA key must be authorized by the management. It is done under dual control, and it is witnessed and signed off by a third person not involved in the actual destruction of the key.

All copies and fragments of the private key are destroyed at the end of the key pair life cycle. If a secure cryptographic device is accessible and known to be permanently removed from service, all private keys stored within the device that have ever been or potentially could be used for any cryptographic purpose are destroyed. If a CA cryptographic device is being permanently removed from service, then any key contained within the device that has been used for any cryptographic purpose is erased from the device. If a CA cryptographic device case is intended to provide tamper-evident characteristics and the device is being permanently removed from service, then the case is destroyed.

For private keys used in conjunction with an HSM, the magnetic storage space that carried the encrypted private key is wiped multiple times to erase any remaining trace and the hardware token (smart card) needed to activate the key is physically destroyed or zeroized, unless it is needed to activate other private keys. If the storage medium itself is replaced (for example, due to hardware failure), it is physically destroyed.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

For private keys stored in encrypted form on the CA system, but which are not protected by an HSM, the magnetic storage space that carried the private key is wiped multiple times to erase any remaining trace. If the storage medium itself is replaced (for example, due to hardware failure), it is physically destroyed.

For private keys stored on a smart card, the private key is destroyed by physically destroying the smart card.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

Any certificate issued by Chosen Security is stored in the certificate repository and on backup media of the systems that host the certificate repository. Chosen Security does not offer any other public key archival service.

6.3.2 Usage periods for the public and private keys

A private key may be used for as long as it is known not to have been compromised and the key parameters are still considered to provide adequate security. Certificates, i. e. signed public keys, may be used for as long as the certificate and / or the repository indicate. Once a certificate has expired, it is no longer valid.

Chosen Security's public and private keys used for issuing certificates in the MBS CMS have a life-time period of at least ten years. The private key's life-time period is lower than that for the corresponding public key, as determined by the validity-period of the certificates that are issued using the private key. If end-entity certificates have a validity period of one year under a certificate policy for which the private key is used to issue certificates, for example, and the life-time period of the CA certificate (and the public key) is ten years, the private key's life-time period is nine years. When the life-time period of the private key ends, key changeover will be initiated (see § 4.7).

6.4 Activation Data

Business requirements for access control are defined and documented in an access control policy which includes identification and authentication process for each user, segregation of duties, and number of persons required to perform specific CA operations (meaning, m of n rule). Activation (and access) data for sensitive keys and assets is under dual control and/or split between at least two disjoint groups of employees.

A formal user registration and deregistration procedure for granting access to activation data for CA information systems and services is followed, and the allocation and use of activation data and privileges is restricted and controlled. Users' access rights are reviewed at regular intervals, and are required to follow defined policies and procedures in the selection and use of passwords.

Subscribers generate their own passwords. It is recommended to select strong passwords.

6.5 Computer Security Controls

A general information security policy document (security policy) is approved by management, published, and communicated, as appropriate, to all employees. This policy is supplemented by detailed policies and procedures for personnel involved in certificate and key management.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

The information security policy contains a definition of information security, its overall objectives and scope, and the importance of security as an enabling mechanism for information sharing. It contains a statement of management intent, supporting the goals and principles of information security, and gives an explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization.

The information security policy lists general and specific responsibilities for information security management, including reporting security incidents, and contains references to documentation which supports the policy. Responsibilities for the protection of individual assets and for carrying out specific security processes are clearly defined. An authorization process for new information processing facilities exists and is followed.

The policies and practices board (see § 8.1) ensures there is clear direction and visible management support for security initiatives. It is responsible for maintaining the security policy and coordinates the implementation of information security measures.

6.6 CA Cryptographic Hardware Life Cycle Controls

Policies and procedures require that CA cryptographic hardware be sent from the manufacturer via registered mail using tamper evident packaging.

Upon the receipt of CA cryptographic hardware from the manufacturer, authorized CA personnel inspect the tamper evident packaging to determine whether the seal is intact. This is followed by acceptance testing and verification of firmware settings.

The cryptographic hardware is then added to an inventory list. To prevent tampering, CA cryptographic hardware is stored in a secure site, with access limited to authorized personnel. Each piece of cryptographic hardware is tracked during its life cycle; any change in its state (removal from storage, integration into the production environment, removal from service etc.) is reflected in an event journal.

The handling, installation and removal of CA cryptographic hardware is performed in the presence of no less than two trusted employees. The same controls apply to service or repair being performed on the CA site. CA cryptographic hardware is never serviced or repaired off-site and subsequently put back into production.

Audit processes and procedures are in place to verify the effectiveness of the controls

6.7 Network Security Controls

Chosen Security has installed adequate protection from both inside and outside attacks (firewalls, intrusion detection mechanisms, virus protection etc.). Computer systems directly involved in issuing certificates have no LAN or WAN connection.

Routing controls are in place to ensure that computer connections and information flows do not breach the access control policy of the organization's business applications.

Networking equipment has turned off all unused network ports and services. Only necessary software is installed on the equipment.

Access to all servers is subject to authentication. Users are provided direct access only to the services that they have been specifically authorized to use.

6.8 Cryptographic Module Engineering Controls

Smart cards used for storing key material are certified according to ITSEC, level "E4 high".

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services
Version 1.2 of January 10, 2007

The Hardware Security Modules used for issuing X.509 certificates meet FIPS 140-1 level 3 (see § 6.2.1).

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services
Version 1.2 of January 10, 2007

7 Certificates and CRL Profiles

7.1 Certificate Profile

7.1.1 Version number(s)

Chosen Security issues X.509 version 3 certificates. X.509 version 1 certificates can be issued upon request.

All certificates issued for the MBA CMS include a reference to the policy OID for this CP/CPS within the appropriate field.

7.1.2 Certificate extensions

Chosen Security uses the standard X.509v3 extensions, in accordance with RFC 2459 and RFC 3280.

The following tables show the minimum extensions for different types of certificates:

CA Certificates:

authorityKeyIdentifier	Non-critical	Identifies the CA certificate that must be used to verify the subscriber's certificate. It contains serial number and issuer DN of the issuing CA certificate
subjectKeyIdentifier	Non-critical	Identifies the CA certificate that must be used to verify the subscriber's certificate. It contains serial number and issuer DN of the issuing CA certificate
basicConstraints	Critical	CA=TRUE
keyUsage	Non-critical	keyCertSign and cRLSign
certificatePolicies	Non-critical	See OID in section Fehler! Verweisquelle konnte nicht gefunden werden. of this CP/CPS
cRLDistributionPoints	Non-critical	location of CRL information
authorityInfoAccess	Non-critical	location of OCSP Responder (only required if OCSP is needed to check revocation status of CA Certificate)

User Certificates

authorityKeyIdentifier	Non-critical	Identifies the CA certificate that must be used to verify the subscriber's certificate. It contains serial number and issuer DN of the
------------------------	--------------	--

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

		issuing CA certificate. The same as subjectKeyIdentifier defined in CA Certificate for CA that issued this User Certificate
subjectKeyIdentifier	Non-critical	
basicConstraints	Critical	
keyUsage	Critical	in accordance with RFC 3280
certificatePolicies	Non-critical	See OID in section Fehler! Verweisquelle konnte nicht gefunden werden. of this CP/CPS
cRLDistributionPoints	Non-critical	location of CRL information
authorityInfoAccess	Non-critical	location of OCSP Responder (only required if OCSP is needed to check revocation status of CA Certificate)

Device Certificates

authorityKeyIdentifier	Non-critical	Identifies the CA certificate that must be used to verify the subscriber's certificate. It contains serial number and issuer DN of the issuing CA certificate. The same as subjectKeyIdentifier defined in CA Certificate for CA that issued this User Certificate
subjectKeyIdentifier	Non-critical	
basicConstraints	Critical	
keyUsage	Critical	in accordance with RFC 3280
extendedKeyUsage	Non-critical	based on device application (e.g., SSL); must adhere to extendedKeyUsage OIDs defined in RFC 3280
certificatePolicies	Non-critical	See OID in section Fehler! Verweisquelle konnte nicht gefunden werden. of this CP/CPS
cRLDistributionPoints	Non-critical	location of CRL information
authorityInfoAccess	Non-critical	location of OCSP Responder (only required if OCSP is needed to check revocation status of CA Certificate)

Chosen Security uses the `ISOAuthorityKeyIdentifier` extension to indicate the CA key that was used to sign the certificate. It contains the serial number and distinguished name of that CA key.

`KeyUsage` is a critical extension and has the value `digitalSignature + nonRepudiation`.

`BasicConstraints` is a critical extension and has the value `false`.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

`SubjectAltName` will be used if the subscriber wishes to include information such as his postal address.

In addition, Chosen Security uses the Microsoft Extensions for Microsoft Authenticode™ (if applicable).

Since extensions are only defined for X.509 version 3 certificates, Chosen Security does not (and cannot) use any extension with X.509 version 1 certificates.

7.1.3 Algorithm object identifiers

Chosen Security currently supports the hash function / digital signature algorithm combinations of `md5withRSAEncryption` and `sha1withRSAEncryption`.

7.1.4 Name forms

See § 3.1.

7.1.5 Name constraints

See § 3.1.

7.1.6 Certificate policy Object Identifier

No stipulation.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical certificate policy extension

If this extension is critical, the certificate path validation software must be able to interpret this extension (including the optional qualifier), or must reject the certificate.

7.2 CRL Profile

Each CRL states the issuer of certificates on the list, the date of issuance, the date of expiry and a list of certificate serial numbers and revoke reasons (unless the latter is unspecified), indicating the certificates issued by the named issuer that have been revoked.

7.2.1 Version number(s)

Chosen Security issues X.509 version 2 CRLs.

7.2.2 CRL and CRL entry extensions

If the key used to sign a CRL is different from the one used to issue certificates on the respective CRL, Chosen Security uses the `authorityKeyIdentifier` to indicate the key

**Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services**

Version 1.2 of January 10, 2007

that was used for issuing certificates on the CRL in question by stating issuer distinguished name and serial number of the certificate issuer certificate.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services
Version 1.2 of January 10, 2007

8 Specific administration

Contact information: see § 1.4

8.1 Specification change procedures

Chosen Security's Policies and Practices board has final authority and responsibility for specifying and approving certification policies, this Certification Practice Statement and Certificate Policy for the Mortgage Bankers Association (CP/CPS). It is responsible for performing a (continuous) assessment to evaluate business risks and determine the security requirements and operational procedures to be included in the applicable documents.

Chosen Security makes available this CP/CPS to all appropriate subscribers and relying parties in the Mortgage Bankers Association CMS. Revisions to this CP/CPS that have significant impact on the users of this CP/CPS must not be made retroactively and shall be published at least two weeks prior to coming into effect.

Revisions to this CP/CPS which are considered to have minimal or no impact on subscribers and relying parties using certificates and CRLs issued by Chosen Security, may be made and posted to the repository without notice to users of the CP/CPS and without changing the version number or date of this CP/CPS.

This version of the CP/CPS is dated January 10, 2007.

8.2 Publication and notification policies

Any time the CP/CPS is amended, and the modified version is approved by the Chosen Security Policies and Practices Board, it is digitally signed and posted to the repository.

8.3 CPS approval procedures

The CP/CPS is reviewed by and accredited by the Chosen Security Policies and Practices Board before being published in the repository.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

9 References

- [RFC2527] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
<ftp://ftp.isi.edu/in-notes/rfc2527.txt>
- [RFC2828] Internet Security Glossary.
<ftp://ftp.isi.edu/in-notes/rfc2828.txt>
- [SIGG] Digital Signature Act (Signaturgesetz - SigG). Article 3 of the Information and Communication Services Act (Informations- und Kommunikationsdienste-Gesetz - IuKDG).
<http://www.iid.de/iukdg/iukdqe.html>
- [SIGV] Digital Signature Ordinance (Signaturverordnung - SigV).
<http://www.iid.de/iukdg/sigve.html>
- [X509] ISO/IEC 9594-8, Information Technology – Open Systems Interconnection – The Directory: Authentication Framework. Also published as ITU-T X.509 Recommendation. See the edition ITU-T Rec. X.509 (1993 E) or ISO/IEC 9594-8:1995 with Technical Corrigendum 1 and Amendment 1 (Certificate Extensions) applied for X.509v3 certificates.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

10 Glossary

A

ACTIVATION DATA

Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e. g., a PIN or a pass phrase).

ASYMMETRIC ALGORITHM

Unlike symmetric algorithms, asymmetric (or public key) encryption algorithms use two different keys for encryption and decryption, where either one cannot be computed from the other.

AUTHENTICATION

Authentication refers to the process of confirming either a person's identity or the integrity of information (or both).

B

BLOCK CIPHER

A block cipher is a symmetric algorithm that encrypts larger blocks of text of fixed size, usually 64 bits (equal to eight characters). Examples of block ciphers are IDEA, DES and Triple-DES. See also stream cipher.

BSI

The BSI is the German government authority for Security in Information Technology. Among other things, it publishes provisions regarding the Digital Signature Act.

C

CA

See Certification Authority.

CERTIFICATE

A certificate is a public key that is signed by a Certification Authority. It binds a public key to the entity named in the certificate (the subject) that holds the corresponding private key. A certificate can be thought of as an electronic ID card. It also identifies the Certification Authority that issued the certificate. The certificate formats most widely used today are PGP and X.509.

CERTIFICATE APPLICATION

In the context of this document, the term "certificate application" refers to all the information a subscriber submits to the Certification Authority in applying for a certificate. This information includes, but may not be limited to, the (digital) certificate request, personal data, a photo-copy of his ID card etc. See also certificate request.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

CERTIFICATE CLASS

Chosen Security issues certificates according to different certificate classes, each of which has a different level of subscriber authentication. See also Certificate Policy.

CERTIFICATE POLICY

A named set of rules that indicates the applicability of a certificate to a particular community and / or class of application with common security requirements. While a CPS is prepared by a Certification Authority, any organization may define a Certificate Policy.

CERTIFICATE POLICY DEFINITIONS

The Chosen Security Certificate Policy Definitions (CPD) is a document describing a set of certificate policies that Chosen Security supports. It is available from the repository.

CERTIFICATE REQUEST

In the context of this document, the term "certificate request" refers to the digitally self-signed public key of the subscriber, which may either be encoded in binary or text form. The certificate request is transformed into a certificate by replacing the owner's signature on the public key with the CA's signature, thereby binding the public key to the entity named in the certificate. See also certificate application.

CERTIFICATE REVOCATION LIST

A list that contains revoked certificates which the CA has issued. If a CA issues certificates under different Certificate Policies, with a different signing key being used for each policy, there will usually be one CRL for each policy, and each of these lists is signed by the private signing key that was used in issuing the certificates on that particular list.

CERTIFICATION AUTHORITY

A Certification Authority is trustworthy institution that certifies public keys, i. e. issues certificates. For this purpose, the information contained in the public key, in particular the key holder's identity, is verified. Chosen Security is an example of a CA.

CERTIFICATION PATH

An ordered sequence of certificates which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

CERTIFICATION PRACTICE STATEMENT

A statement of the practices which a Certification Authority employs in issuing certificates. See also Certificate Policy.

CERTIFICATION SERVICES PROVIDER

A Certification Services Provider is a third party that manages any of the services that a Certification Authority generally provides, such as issuing certificates, a directory service, an online certificate status responder or end entity registration.

CERTIFY

To digitally sign another entity's public key by using one's own private key.

CIPHER

A cipher is a cryptographic algorithm used for encryption.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

CMS CUSTOMER

A customer which has entered into a contract with Chosen Security to render Mortgage Industry CMS.

CONFIRM

To ascertain through appropriate inquiry and investigation.

CONVENTIONAL ALGORITHMS

See symmetric algorithms.

CORRESPOND

To belong to the same key pair.

CPD

See Certificate Policy Definitions.

CPS

See Certification Practice Statement.

CRL

See Certificate Revocation List.

CRYPTANALYSIS

Cryptanalysis deals with the breaking of encryption algorithms, i. e. decrypting coded messages.

CRYPTOGRAPHY

Cryptography is the science of keeping messages secret.

CRYPTOLOGY

Cryptology is the area of mathematics that combines cryptography and cryptanalysis.

[CSP]

See Certification Services Provider.

D

DECRYPTION

The process of unscrambling encrypted data.

DES

DES (Data Encryption Standard) is a block cipher developed by IBM in the early 1970s. Initially, the key size used in the algorithm was 128 bits, but the NSA reduced it to 56 bits, which is considered too weak nowadays. A DES variant known as Triple DES offers better security.

DH

See Diffie-Hellman.

DIFFIE-HELLMAN

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

Diffie-Hellman is a secure public key exchange algorithm invented by Whitfield Diffie and Martin Hellman in 1976. The Diffie-Hellman patent expired in 1997.

DIGITAL CERTIFICATE

See certificate.

DIGITAL SIGNATURE

A digital signature is a small block of data (hash value) that is encrypted using the sender's private key and appended to the signed data to provide authenticity and integrity. The digital signature is checked using the sender's public key.

DIGITAL SIGNATURE ACT

The German Digital Signature Act (SigG) and the Digital Signature Ordinance (SigV) aim "to establish general conditions under which digital signatures are deemed secure and forgeries of digital signatures or manipulation of signed data can be reliably ascertained." It came into force on August 1st, 1997. A revision that reflects the experiences gained thus far, and implements Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, is expected to be enacted in the second quarter of 2001.

DISTINGUISHED NAME

Strictly speaking, a Distinguished Name (DN) is a path through an X.500 directory information tree which uniquely identifies an entity. An X.500 directory tree is a hierarchical structure, and because information like an e-mail address follows no such hierarchy, it should not be part of a DN. Most DNs do, however, contain an e-mail address, and a DN is commonly understood to be comprised of the collection of data fields that make up a standard X.509, i. e., Country (C), State / Province (SP), Locality (L), Organization (O), Organizational Unit (OU), Common Name (CN) and Email. A DN following this scheme might look like the following: /C=US/SP=Washington/L=Seattle/O=My Company, Inc. /OU=Internet Services/CN=John Doe/Email=jdoe@mycompany.com.

DN

See Distinguished Name.

DSA

A public key signature algorithm proposed by NIST for use in DSS that uses a variable key size from 512 to 1024 bits.

DSS

DSS (Digital Signature Standard) is a digital signature standard proposed by NIST. DSS is used, for instance, by PGP version 5.0 and above.

E

ENCRYPTION

The process of scrambling and rendering data useless for anyone other than the intended recipient.

ENTITY

See person.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

F

FINGERPRINT

The fingerprint is an extract of the public key (usually 128 or 160 bits in size) that is used to readily verify that one has the correct key, i. e. that the key belongs to the entity named in the certificate, without having to check that the entire key (usually 1024 bits and above) matches exactly. It is computed by applying a hash function to the public key.

H

HASH FUNCTION

A hash function generates a short extract of fixed length (MD5: 128 bits = 16 characters, SHA-1: 160 bits = 20 characters), the hash value, from any given data in such a way that the original data cannot be derived from the extract, and that it is infeasible to construct other data that produces the same hash value. For example, the hash value derived by applying the hash function to the body (the message text) of an e-mail is then encrypted using the private key in order to digitally sign the e-mail.

HYBRID ALGORITHMS

A hybrid encryption algorithm combines symmetric and asymmetric algorithms in order to make use of their respective advantages, higher speed (symmetric) and easier key exchange (asymmetric).

I-J

IDEA

IDEA (International Data Encryption Algorithm) is a 64 bit block cipher that uses a 128 bit key. IDEA is considered to be one of the most secure encryption algorithms. It is used (among others) by PGP. Commercial users of PGP that use IDEA as the symmetric cipher have to pay a license fee to the Swiss company ASCOM; non-commercial use is free of charge.

IETF

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.

ISSUE A CERTIFICATE

The process of a CA signing an end user's public key, thus creating the certificate, and notifying the subscriber of its contents.

K

KEY

A digital code used to encrypt, decrypt, create and verify digital signatures. Keys used for asymmetric algorithms come in pairs, and anything encrypted with either one of them must be decrypted with the other. Symmetric algorithms, however, use the same key for both encryption and decryption, and there is no concept of a digital signature.

KEY PAIR

The set of keys used for asymmetric algorithms. See also key.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

KEY RING

The key ring is the file PGP keeps the public (or private) keys in.

L

LAN

Local Area Network.

LDAP

A protocol for accessing on-line directory services. LDAP was defined by the IETF in order to encourage adoption of X.500 directories. The Directory Access Protocol (DAP) was seen as too complex for simple Internet clients to use. An LDAP directory entry is a collection of attributes with a name, called a distinguished name (DN). The DN refers to the entry unambiguously. Each of the entry's attributes has a type and one or more values. The types are typically mnemonic strings, like "CN" for common name, or "mail" for e-mail address. The values depend on the type. For example, a mail attribute might contain the value "john.doe@company.com". LDAP directory entries are arranged in a hierarchical structure that reflects political, geographic, and / or organizational boundaries.

M

MD5

MD5 is a 128 bit hash function developed by Ron Rivest. It is widely used, and PGP uses it in conjunction with the RSA algorithm. Since MD5 has been found to have weaknesses, SHA-1 is to be preferred, although these weaknesses are hard to exploit in practice.

N

NIST

The NIST (National Institute for Standards and Technology) is a branch of the US Department of Commerce that proposes open interoperability standards.

NSA

The NSA (National Security Agency) is a cryptologic organization of the US government that deals with the development and the cryptanalysis of encryption algorithms.

O

ONE-WAY FUNCTION

See hash function.

P

PASS PHRASE

A pass phrase, just like a pass word, is used to deny unauthorized access to confidential data. A pass phrase consists of several words, punctuation marks and numbers to provide better security than a simple pass word. A pass phrase is used, for instance, to protect the private key.

PEM

PEM (Privacy-Enhanced Mail) is an Internet mail standard that implements protocols for encryption, message integrity, key management and authentication (see digital signature).

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

PEM uses RSA keys ranging from 508 to 1024 bits. PEM certificates are based on the X.509 format.

PERSON

A human being or any organization capable of signing a document, either legally or as a matter of fact.

PGP

PGP (Pretty Good Privacy), developed by Phillip Zimmermann, is a popular and very widely used application for exchanging secure e-mail and encrypting files. Non-commercial use is free, commercial users will have to obtain a license from PGP Inc., now owned by Network Associates Inc.

PIN

Personal Identification Number.

PRIVATE KEY

Of the key pair used in asymmetric algorithms, the private key is the one that must be kept secure by its owner. No one else must have access to this key. Usually, the private key is protected by a pass word or a pass phrase. It is used for decrypting messages sent to the owner of the corresponding public key and for generating digital signatures.

PUBLIC KEY

Of the key pair used in asymmetric algorithms, the public key is the one that is made publicly available, e. g. on a public key server. Its purpose is to encrypt messages sent to the key owner and to verify digital signatures that the latter has made using the corresponding private key. A public key certified by a Certification Authority is called a certificate.

PUBLIC KEY ENCRYPTION ALGORITHM

See asymmetric algorithm.

PUBLIC KEY EXCHANGE ALGORITHM

A public key method for exchanging session keys. Most public key algorithms are simply used for exchanging secret keys for symmetric encryption algorithms, not for encryption of data. Diffie-Hellman is suitable for key exchange only, while RSA is a public key encryption algorithm.

PUBLIC KEY SERVER

A public key server is a public key directory, much like a public telephone book, which lists user names and their public keys for easy access.

Q-R

RA

See Registration Authority.

REGISTRATION AUTHORITY

An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates, i. e., an RA is delegated certain tasks on behalf of a CA.

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

RELYING PARTY

A recipient of a certificate who acts in reliance on that certificate and / or digital signatures verified using that certificate.

REPOSITORY

A collection of databases for storing and retrieving certificates, CRLs and any other information related to certificates and digital signatures, for example this CP/CPS.

REVOCATION

Revocation is the process of declaring one's public key as no longer valid. This is normally done because its owner can no longer guarantee that he has sole access, and that his private key has not been compromised. By revoking the corresponding public key one aims to prevent others from doing any damage by pretending to be the key's owner. Revoking the key lets people know that the public key should no longer be used to encrypt any messages or files, and that digital signatures made using this key should no longer be accepted. The revoked key is then placed on a CRL (Certificate Revocation List) by a Certification Authority so that anyone can check whether a public key is still valid.

RSA

RSA is the name of the asymmetric algorithm developed by the US-based company of the same name, RSA Data Security Inc. Its security is based on the fact that it is easy to multiply two large primes (with several hundred decimal digits each) but very hard to factor them out of the product. The abbreviation RSA refers to the three inventors of the algorithm: Ron Rivest, Adi Shamir und Leonard Adleman.

S

SECRET KEY

See private key.

SECRET KEY ALGORITHM

See symmetric algorithm.

SELF-SIGNED

A public key is referred to as self-signed if it is digitally signed using the corresponding private key.

SESSION KEY

In hybrid algorithms, the key used for the symmetric encryption algorithm and exchanged via the public key algorithm. The session key is randomly generated for each exchange of data, i.e. for each session, while the public key remains the same over a longer period of time.

SET OF PROVISIONS

A collection of practice and / or policy statements, spanning a range of standard topics, for use in expressing a certificate policy definition or CPS.

SHA-1

SHA-1 is a 160 bit hash function developed by NIST that is used in the DSS.

SIGG

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

See Digital Signature Act.

SIGV

See Digital Signature Act.

S/MIME

S/MIME (Secure Multipurpose Mail Extension) is a standard suggested by a group of software developers lead by RSADSI that provides encryption and digital signatures for exchanging secure e-mail. S/MIME certificates are based on the X.509 format.

SSL

SSL (Secure Socket Layer) is a protocol developed by Netscape that aims to provide secure data exchange over the Internet. SSL is supported and used by all modern Internet browsers in order to protect the communication and the transfer of sensitive data on the world wide Web through encryption. Unfortunately, the export versions of these applications that are available outside of the United States are limited to a weak 40 bit encryption (instead of 128 bit) due to export restrictions. SSL certificates are based on the X.509 format.

STEGANOGRAPHY

In contrast to cryptography, steganography aims to conceal that there actually is any secret message by hiding the confidential message in other data (e. g. in a digital image).

STREAM CIPHER

A stream cipher is a symmetric algorithm that encrypts the message character by character. See also block cipher.

SUBSCRIBER

A person that is the subject named in a certificate and holds the private key corresponding to the public key listed in the certificate.

SUSPENSION

Suspension is the process of placing one's certificate on hold, i. e., declaring it as temporarily invalid. This is normally done because the subscriber suspects that his private key has been lost or compromised. By suspending the corresponding public key one aims to prevent others from doing any damage by pretending to be the key's owner. Suspending the key lets people know that, for the time being, the public key should not be used to encrypt any messages or files, and that digital signatures made using this key should not be accepted at the moment. A suspended key must either be revoked upon confirming that the private key has indeed been lost or compromised, when it is placed on a CRL (Certificate Revocation List) by the issuing Certification Authority, or the suspension may be lifted, if, for example, the private key has been recovered (i. e., is not lost).

SYMMETRIC ALGORITHM

In contrast to asymmetric algorithms, the key used for decryption (or encryption) can be computed from the other key in a symmetric (or conventional) encryption algorithm. Most of the time both keys are the same.

T

TIME-STAMP

Chosen Security and TC TrustCenter
Certificate Policy and Certification Practice Statement
for Mortgage Industry Certificate Management Services

Version 1.2 of January 10, 2007

An indication of (at least) the date and time a document was signed and by whom.

TRIPLE-DES

A variant of the DES algorithm where DES (key size 56 bits) is used three times with three different keys. The effective key size is only 112 bits (and not 168 bits, as one might expect).

U-V

USER ID

A PGP data structure containing the key owner's identity. The commonly used format is "Full name <e-mail address>", e. g. "John Doe <jdoe@company.com>".

W-Z

WAN

Wide Area Network.

X.509

X.509 is a standard certificate format of the ITU-T (International Telecommunication Union-Telecommunication). It contains the name of the issuer, usually a Certification Authority, information about the key owner's identity and the digital signature of the issuer. Both SSL and S/MIME are based on the X.509 format.