Advantage Security Certification Practice Statement

Version 3.8.5

Effective Date: 01/01/2012

Advantage Security

-

1. INTRODUCTION

This document is the [Advantage Security] Certification Practice Statement (ñCPSò). It states the practices that Advantage Security certification authorities (ñCAsò) employ in providing certification

1.3

Table 7. Authentication of individual identity

3.2.4

3.3.1 Identification and Authentication for Routine Re-key

Re-key procedures ensure that the person or organization seeking to rekey an end-user Subscriber Certificate is in fact the Subscriber of the Certificate.

One acceptable procedure is through the use of a Chall ge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscrib1 0 0 1 398.8 choose and submit with their enrol ent information a Chall nge Phrase. Upon renewal a Certificat1 0, if a Subscriber correctly submits

4.1.2

4.3

Reliance on a certificate must be reasonable under the circumstances. If the circumstances

4.7 *Certificate Re-Key*

Certificate rekey is the application for the issuance of a new certificate that certifies the new public key. Certificate rekey is supported for all certificate Classes.

4.7.1 Circumstances for Certificate Re-Key

Prior to the expiration of an existing Subscriberõs Certificate, it is necessary for the Subscriber to re-key the certificate to maintain continuity of Certificate usage. A certificate may also be re-keyed after expiration.

4.7.2 Who May Request Certification of a New Public Key

Only the subscriber for an individual certificate or an authorized representative for an Organizational certificate may request certificate renewal

4.7.3 Processing Certificate Re-Keying Requests

Re-key

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

4.8 *Certificate Modification*

4.8.1 Circumstances for Certificate Modification

Certificate modification refers to the application for the issuance of a new certificate due to

Advantage Security or

CRLs for Authenticated Content Signing (ACS) R

customer may use KMS operated either out of the enterpqiseô s pn ise[Affiliateô] secure data center. If operated out of the enterp! eô s p! Aiseantage Security does not store copies of Subscriber private keys but plays an important role in the Subscriber key recovery process.

4.12.1 Key Escrow and Recovery Policy and Practices

Enterprise customers using the Managed PKI Key Management service (or an equivalent service approved by Symantec) are permitted to escrow end-

5.1.3 Power and Air Conditioning

Advantage Security

- ¶ cryptographic business operations personnel,
- ¶ security personnel,
- ¶ system administration personnel,
- ¶ designated engineering personnel, and
- ¶ executives that are designated to manage infrastructural trustworthiness.

Advantage Security considers the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requireme4(d)ss set out in this CPS.

5.2.2 Number of 0 -3(e)-3(rs)-4(on)12(s)-3(R)10(e)-3(quire)-4(d)]TJETBT1 0 0 1 292.13 590.02

two (2) authorized Administrators

5.2.3 Identification and Authentication for Each Ro

For all personnel seeking to become Trusted Persons, verification of identity is performed through

- ¶ the acceptance, rejection, or other processing of Certificate Applications, revocation requests, recovery requests or renewal requests, or enrollment information;
- ¶ the issuance, or revocation of Certificates, including personnel having access to restricted portions of the repository;
- ¶ the handling of Subscriber information or requests
- ¶ the generation, issuing or destruction of a CA certificate
- ¶ the loading of a CA to a Production environment

5.3 *Personnel Controls*

Personnel seeking to become Trusted Persons must present proof of the requisite background, qualifications, and experien8.38 Tobded to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts. B1 0 0 1 90.024 613.06 T chec90.024s are repeated at least every 5 years for personnel holding Trusted Positions.

5.3.1 Qualifications, Experience, and Clearance Requirements

Advantag3(l)5 Securityqlre s that plonnel seeking to become Trusted Persons present proof of the reqls0.024ite bac90.024ground, qllifications, and experience needed to perform their prospective job

5.4 *Audit Logging Procedures*

5.4.1 Types of Events Recorded

Advantage Security

5.4.4 Protection of Audit Log

Audit logs are protected with an electronic audit log system that includes mechanisms to protect

5.5.4 Archive Backup Procedures

Advantage Security incrementally backs up electronic archives of its issued Certificate

6.2.1 Cryptographic Module Standards and Controls

For PCA and Issuing Root CA key pair generation and CA private key storage, Advantage Security uses hardware cryptographic modules that are certified at or meet the requirements of FIPS 140-1 Level 3.

6.2.2 Private Key (m out of n) Multi-Person Control

Advantage Security has implemented technical and procedural mechanisms that require the

6.2.8.4

Where required, Advantage Security destroys CA private keys in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key. Advantage Security utilizes the zeroization function of its hardware cryptographic modules

access to production servers to those individuals with a valid business reason for such access. General application users do not have accounts on production servers.

Advantage Securityôs production network is logl cally sparated from otr c

6.8 *Time-Stamping*

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be

7. Certificate, CRL, and O' C Profiles

7.1 *Certificate Profile*

Advantage Security generally conform to (a) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - Th9-7(V(i)5(r)-3(ec)-3toer)-15(y)18:t Ah9-7nati-cation

- Class 2 Enterprise certificates and Class 3 organization certificates using the Symantec

9.2.3 Extended Warranty Coverage

No Stipulation

9.3 ***Confidentiality of Business Information***

9.3.1 Scope of Confidential Information

9.4.4 Responsibility to Protect Private Information

STN

9.5.4 Property Rights in Keys and Key Material

Key pairs corresponding to Certificates of CAs and end-user Subscribers are the property of the CAs and end-user Subscribers that are the respective Subjects of these Certificates, subject to the rights of enterprise Customers using Managed PKI Key Manager, regardless of the physical medium within which they are stored and protected, and such persons retain all Intellectual Property Rights in and to these key pairs. Without limiting the generality of the foregoing, Symantec

¶ All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true,
¶ All information supplied by the Subscriber and contain3(u)-dine3(e)rtificate is true,
¶ The Certificate is being used exclusivel4(x)-55.02 TmFr(r)-11(u8(e 7Frie i)z)-9(d Cert(d)-9((the)l)-9(d b)ga)-6(i)

x

9.9 *Indemnities*

9.9.1 Indemnification by Subscribers

To the extent permitted by applicable law, Subscribers are required to indemnify Advantage Security for:

¶

9.12 *Amendments*

9.12.1 Procedure for Amendment

Amendments to this CPS may be made by the Advantage Security