**CÔNG TY CỔ PHẦN HỖ TRỢ DOANH NGHIỆP VÀ ĐẦU TƯ HN**

**DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ**

**NC – CA**

**\*\*\*\*\***

**QUY CHẾ CHỨNG THỰC**

**Certificate Policy (CP) & Certificate Practices Statement (CPS)**

**Hà Nội, 11-2019NỘI DUNG**

[I GIỚI THIỆU 9](#_Toc8997794)

[I.1 Giới thiệu về Quy chế chứng thực 9](#_Toc8997795)

[I.2 Tên và định danh của tài liệu 10](#_Toc8997796)

[I.3 Thành viên tham gia hệ thống PKI công cộng 10](#_Toc8997797)

[I.3.1 RootCA 10](#_Toc8997798)

[I.3.2 NC-CA 10](#_Toc8997799)

[I.3.3 Thuê bao 11](#_Toc8997800)

[I.3.4 Đại lý 11](#_Toc8997801)

[I.3.5 Bên tin tưởng 12](#_Toc8997802)

[I.3.6 Các đối tượng khác 12](#_Toc8997803)

[I.4 Phương thức sử dụng chứng thư số 12](#_Toc8997804)

[I.4.1 Phạm vi sử dụng 12](#_Toc8997805)

[I.4.2 Cấm sử dụng 13](#_Toc8997806)

[I.5 Tổ chức quản lý chính sách 13](#_Toc8997807)

[I.5.1 Tổ chức quản trị tài liệu 13](#_Toc8997808)

[I.5.2 Người liên hệ 13](#_Toc8997809)

[I.5.3 Người quyết định sự phù hợp của Quy chế chứng thực chữ ký số 14](#_Toc8997810)

[I.5.4 Tổ chức phê chuẩn quy chế chứng thực 14](#_Toc8997811)

[I.5.5 Thủ tục phê chuẩn quy chế chứng thực 14](#_Toc8997812)

[I.6 Định nghĩa và viết tắt 14](#_Toc8997813)

[II TRÁCH NHIỆM VỀ CÔNG BỐ VÀ LƯU TRỮ 17](#_Toc8997814)

[II.1 Kho lưu trữ 17](#_Toc8997815)

[II.2 Công bố thông tin về chứng thư số 17](#_Toc8997816)

[II.3 Thông tin về tần suất công bố 17](#_Toc8997817)

[II.4 Kiểm soát truy cập vào kho lưu trữ 18](#_Toc8997818)

[III ĐỊNH DANH VÀ XÁC THỰC 18](#_Toc8997819)

[III.1 Đặt tên 18](#_Toc8997820)

[III.1.1 Phân loại 18](#_Toc8997821)

[III.1.2 Quy định đặt tên 18](#_Toc8997822)

[III.1.3 Biệt hiệu hay nặc danh 20](#_Toc8997823)

[III.1.4 Tính duy nhất của tên 20](#_Toc8997824)

[III.1.5 Chấp nhận, xác thực và vai trò của nhãn hiệu đăng ký (TradeMarks) 20](#_Toc8997825)

[III.2 Xác minh khi cấp chứng thư số lần đầu 21](#_Toc8997826)

[III.2.1 Phương pháp chứng minh sở hữu khóa riêng 21](#_Toc8997827)

[III.2.2 Kiểm tra nhận dạng thông tin của tổ chức doanh nghiệp 21](#_Toc8997828)

[III.2.3 Xác thực nhận dạng thông tin của cá nhân 22](#_Toc8997829)

[III.2.4 Xác thực danh tính tên miền hoặc thiết bị 22](#_Toc8997830)

[III.2.5 Trường hơp thuê bao tự tạo cặp khóa 23](#_Toc8997831)

[III.2.6 Thông tin không xác minh 23](#_Toc8997832)

[III.2.7 Xác minh ủy quyền 23](#_Toc8997833)

[III.2.8 Tiêu chuẩn tích hợp 23](#_Toc8997834)

[III.3 Định danh và xác thực khi yêu cầu thay đổi khóa 23](#_Toc8997835)

[III.3.1 Định danh và xác thực khi yêu cầu thay đổi khóa 23](#_Toc8997836)

[III.3.2 Nhận dạng và xác thực yêu cầu gia hạn chứng thư số 24](#_Toc8997837)

[III.4 Định danh và xác thực khi yêu cầu thu hồi chứng thư số 24](#_Toc8997838)

[IV YÊU CẦU VẬN HÀNH VỀ VÒNG ĐỜI CHỨNG THƯ SỐ 25](#_Toc8997839)

[IV.1 Đăng ký chứng thư số 25](#_Toc8997840)

[IV.1.1 Các đối tượng có thể xin cấp chứng thư số 25](#_Toc8997841)

[IV.1.2 Hồ sơ xin cấp chứng thư bao gồm: 25](#_Toc8997842)

[IV.1.3 Đăng ký cấp chứng thư số và trách nhiệm của các bên 25](#_Toc8997843)

[IV.2 Xử lý hồ sơ đăng ký chứng thư số 28](#_Toc8997844)

[IV.2.1 Nhận dạng và xác thực 28](#_Toc8997845)

[IV.2.2 Duyệt đăng ký cấp chứng thư số 28](#_Toc8997846)

[IV.2.3 Thời gian xử lý đăng ký cấp chứng thư số 28](#_Toc8997847)

[IV.3 Cấp chứng thư số 29](#_Toc8997848)

[IV.3.1 Thuê bao đăng ký cấp chứng thư số 29](#_Toc8997849)

[IV.3.2 NC-CA tạo chứng thư số 29](#_Toc8997850)

[IV.3.3 Thông báo cho thuê bao khi đã tạo xong chứng thư số 29](#_Toc8997851)

[IV.4 Chấp nhận chứng thư số 29](#_Toc8997852)

[IV.4.1 Tổ chức bàn giao và xác nhận 29](#_Toc8997853)

[IV.4.2 Công bố chứng thư số 30](#_Toc8997854)

[IV.4.3 Thông báo sự ban hành chứng thư số 30](#_Toc8997855)

[IV.5 Sử dụng chứng thư số và cặp khóa 30](#_Toc8997856)

[IV.5.1 Sử dụng khóa bí mật và chứng thư số 30](#_Toc8997857)

[IV.5.2 Sử dụng khóa công khai và chứng thư số 30](#_Toc8997858)

[IV.6 Gia hạn chứng thư số 31](#_Toc8997859)

[IV.6.1 Các tình huống gia hạn chứng thư số 33](#_Toc8997860)

[IV.6.2 Đối tượng có thể yêu cầu gia hạn chứng thư số 33](#_Toc8997861)

[IV.6.3 Xử lý yêu cầu gia hạn chứng thư số 33](#_Toc8997862)

[IV.6.4 Thông báo sự tạo chứng thư số mới cho thuê bao 33](#_Toc8997863)

[IV.6.5 Bàn giao và xác nhận với thuê bao 34](#_Toc8997864)

[IV.6.6 Công bố chứng thư số mới được gia hạn 34](#_Toc8997865)

[IV.6.7 Thông báo tạo chứng thư số mới được gia hạn cho các đối tượng khác 34](#_Toc8997866)

[IV.7 Thay đổi khóa chứng thư số 34](#_Toc8997867)

[IV.7.1 Các trường hợp thay đổi khóa chứng thư số 34](#_Toc8997868)

[IV.7.2 Người yêu cầu thay đổi khóa chứng thư số 34](#_Toc8997869)

[IV.7.3 Quy trình xử lý yêu cầu thay đổi khóa chứng thư số 34](#_Toc8997870)

[IV.7.4 Thông báo cho thuê bao 34](#_Toc8997871)

[IV.7.5 Bàn giao và xác nhận với thuê bao 35](#_Toc8997872)

[IV.7.6 Công bố chứng thư số 35](#_Toc8997873)

[IV.7.7 Thông báo việc thay đổi khóa chứng thư số của thuê bao đến các tổ chức, cá nhân khác 35](#_Toc8997874)

[IV.8 Thay đổi thông tin chứng thư số 35](#_Toc8997875)

[IV.8.1 Các trường hợp thay đổi chứng thư số 35](#_Toc8997876)

[IV.8.2 Người yêu cầu thay đổi chứng thư số 35](#_Toc8997877)

[IV.8.3 Quy trình xử lý yêu cầu thay đổi chứng thư số 35](#_Toc8997878)

[IV.8.4 Thông báo cho thuê bao 36](#_Toc8997879)

[IV.8.5 Bàn giao và xác nhận với thuê bao 36](#_Toc8997880)

[IV.8.6 Công bố chứng thư số 36](#_Toc8997881)

[IV.8.7 Thông báo việc thay đổi chứng thư số của thuê bao đến các tổ chức, cá nhân khác 36](#_Toc8997882)

[IV.9 Thu hồi và đình chỉ chứng thư số 36](#_Toc8997883)

[IV.9.1 Các tình huống thu hồi chứng thư số 36](#_Toc8997884)

[IV.9.2 Ai có thể yêu cầu thu hồi chứng thư số 37](#_Toc8997885)

[IV.9.3 Thủ tục thu hồi chứng thư số 37](#_Toc8997886)

[IV.9.4 Thủ tục thu hồi chứng thư số 37](#_Toc8997887)

[IV.9.5 Thời hạn gửi yêu cầu thu hồi chứng thư số 38](#_Toc8997888)

[IV.9.6 Thời gian bắt đầu xử lý yêu cầu thu hồi chứng thư số 38](#_Toc8997889)

[IV.9.7 Kiểm tra trạng thái thu hồi 38](#_Toc8997890)

[IV.9.8 Tần suất công bố CRL mới 39](#_Toc8997891)

[IV.9.9 Kiểm tra trạng thái chứng thư số trực tuyến 39](#_Toc8997892)

[IV.9.10 Yêu cầu kiểm tra trạng thái thu hồi trực tuyến 39](#_Toc8997893)

[IV.9.11 Các dạng thông tin trạng thái thu hồi khác 39](#_Toc8997894)

[IV.9.12 Quy trình tạm dừng chứng thư số 39](#_Toc8997895)

[IV.9.13 Quy trình phục hồi chứng thư số 39](#_Toc8997896)

[IV.9.14 Yêu cầu đặc biệt khi khóa CA, sub CA bị mất, bị lộ hoặc thu hồi 39](#_Toc8997897)

[IV.10 Dịch vụ về trạng thái chứng thư số 39](#_Toc8997898)

[IV.10.1 Phương tiện công bố 39](#_Toc8997899)

[IV.10.2 Tính sẵn sàng của dịch vụ 39](#_Toc8997900)

[IV.10.3 Tùy chọn đặc biệt 40](#_Toc8997901)

[IV.11 Kết thúc thuê bao chứng thư số 40](#_Toc8997902)

[IV.12 Lưu khóa ở bên thứ ba và khôi phục khóa 40](#_Toc8997903)

[IV.12.1 Chính sách và thủ tục gửi giữ khóa riêng 40](#_Toc8997904)

[IV.12.2 Chính sách và thủ tục khôi phục gửi giữ khóa riêng 40](#_Toc8997905)

[V THIẾT BỊ, QUẢN LÝ VÀ KIỂM SOÁT VẬN HÀNH 41](#_Toc8997906)

[V.1 Kiểm soát vật lý 41](#_Toc8997907)

[V.1.1 Địa điểm đặt hệ thống 41](#_Toc8997908)

[V.1.2 Truy cập vật lý 41](#_Toc8997909)

[V.1.3 Điều kiện về nguồn điện, môi trường và phòng tránh thảm họa 42](#_Toc8997910)

[V.1.4 Phương án phòng chống thiên tai 42](#_Toc8997911)

[V.1.5 Phương án phòng cháy chữa cháy 43](#_Toc8997912)

[V.1.6 Phương tiện lưu trữ dữ liệu 43](#_Toc8997913)

[V.1.7 Xử lý rác 43](#_Toc8997914)

[V.1.8 Hệ thống dự phòng ở địa điểm khác 43](#_Toc8997915)

[V.2 Các thủ tục kiểm soát 43](#_Toc8997916)

[V.2.1 Những cá nhân được tin tưởng 43](#_Toc8997917)

[V.2.2 Số người được yêu cầu trên một nhiệm vụ nhạy cảm 44](#_Toc8997918)

[V.2.3 Nhận dạng và xác thực trong mỗi vai trò 44](#_Toc8997919)

[V.2.4 Những vai trò yêu cầu phải phân tách nhiệm vụ 44](#_Toc8997920)

[V.3 Kiểm soát nhân sự 45](#_Toc8997921)

[V.3.1 Khả năng chuyên môn, kinh nghiệm và sự trong sạch 45](#_Toc8997922)

[V.3.2 Các thủ tục kiểm tra lý lịch, trình độ 45](#_Toc8997923)

[V.3.3 Yêu cầu đào tạo vận hành hệ thống 45](#_Toc8997924)

[V.3.4 Nhu cầu và tần suất đào tạo 46](#_Toc8997925)

[V.3.5 Tần suất luân chuyển công việc 46](#_Toc8997926)

[V.3.6 Xử phạt các hành động không được phép 46](#_Toc8997927)

[V.3.7 Yêu cầu đối với nhà thầu 46](#_Toc8997928)

[V.3.8 Tài liệu cấp cho cán bộ 46](#_Toc8997929)

[V.3.9 Phối hợp với Trung tâm Chứng thực điện tử quốc gia 46](#_Toc8997930)

[V.4 Quy trình lưu nhật ký kiểm toán hệ thống NC-CA 47](#_Toc8997931)

[V.4.1 Các loại sự kiện được ghi lại 47](#_Toc8997932)

[V.4.2 Tần suất xử lý nhật ký kiểm toán 47](#_Toc8997933)

[V.4.3 Thời hạn giữ lại các nhật ký kiểm toán 47](#_Toc8997934)

[V.4.4 Bảo vệ các nhật ký kiểm toán 48](#_Toc8997935)

[V.4.5 Các thủ tục dự phòng nhật ký kiểm toán 48](#_Toc8997936)

[V.4.6 Phương thức ghi nhật ký kiểm toán 48](#_Toc8997937)

[V.4.7 Thông báo cho đối tượng gây ra sự kiện 48](#_Toc8997938)

[V.4.8 Đánh giá lỗ hổng hệ thống 48](#_Toc8997939)

[V.5 Lưu trữ các bản ghi 48](#_Toc8997940)

[V.5.1 Các loại bản ghi được lưu trữ 48](#_Toc8997941)

[V.5.2 Thời hạn giữ lại các lưu trữ 48](#_Toc8997942)

[V.5.3 Bảo vệ lưu trữ 49](#_Toc8997943)

[V.5.4 Các thủ tục sao lưu lưu trữ 49](#_Toc8997944)

[V.5.5 Nhãn thời gian của các bản ghi 49](#_Toc8997945)

[V.5.6 Hệ thống lưu trữ 49](#_Toc8997946)

[V.5.7 Thủ tục truy cập và kiểm tra thông tin lưu trữ 49](#_Toc8997947)

[V.6 Thay đổi khóa của NC-CA 49](#_Toc8997948)

[V.7 Lộ khóa và khôi phục sự cố/thảm họa 50](#_Toc8997949)

[V.7.1 Các thủ tục kiểm soát sự cố và thảm họa 50](#_Toc8997950)

[V.7.2 Sự cố về máy tính, phần mềm và dữ liệu 50](#_Toc8997951)

[V.7.3 Thủ tục xử lý khi khóa bí mật bị làm mất/lộ 50](#_Toc8997952)

[V.7.4 Khả năng phục hồi hoạt động sau thảm họa 51](#_Toc8997953)

[V.8 Kết thúc CA và RA 51](#_Toc8997954)

[VI KIỂM SOÁT AN TOÀN KỸ THUẬT 52](#_Toc8997955)

[VI.1 Tạo cặp khóa và cài đặt 52](#_Toc8997956)

[VI.1.1 Sinh cặp khóa 52](#_Toc8997957)

[VI.1.2 Chuyển giao khóa bí mật cho khách hàng 52](#_Toc8997958)

[VI.1.3 Chuyển giao khóa công khai của thuê bao đến NC-CA 52](#_Toc8997959)

[VI.1.4 Công bố chứng thư số của NC-CA 52](#_Toc8997960)

[VI.1.5 Độ dài khóa 52](#_Toc8997961)

[VI.1.6 Các tham số sinh cặp khóa mã công khai và kiểm tra chất lượng 53](#_Toc8997962)

[VI.1.7 Mục đích sử dụng khóa (theo X.509 V3) 53](#_Toc8997963)

[VI.2 Bảo vệ khóa bí mật và kiểm soát module mã hóa 53](#_Toc8997964)

[VI.2.1 Tiêu chuẩn module mã hóa 53](#_Toc8997965)

[VI.2.2 Lưu giữ ngoài khóa bí mật của thuê bao 53](#_Toc8997966)

[VI.2.3 Cơ chế kiểm soát khóa bí mật 53](#_Toc8997967)

[VI.2.4 Dự phòng khóa bí mật 53](#_Toc8997968)

[VI.2.5 Lưu trữ khóa bí mật 54](#_Toc8997969)

[VI.2.6 Chuyển khóa bí mật vào/ra HSM 54](#_Toc8997970)

[VI.2.7 Phương pháp giữ khóa riêng NC-CA 54](#_Toc8997971)

[VI.2.8 Phương thức kích hoạt khóa bí mật 54](#_Toc8997972)

[VI.2.9 Phương pháp ngừng kích hoạt khóa bí mật 54](#_Toc8997973)

[VI.2.10 Phương pháp hủy bỏ khóa bí mật 54](#_Toc8997974)

[VI.2.11 Đánh giá thiết bị mã hóa phần cứng 55](#_Toc8997975)

[VI.3 Các vấn đề khác của việc quản lý cặp khóa 55](#_Toc8997976)

[VI.3.1 Lưu trữ khóa công khai 55](#_Toc8997977)

[VI.3.2 Thời hạn sử dụng chứng thư số và thời hạn sử dụng cặp khóa 55](#_Toc8997978)

[VI.4 Dữ liệu kích hoạt 55](#_Toc8997979)

[VI.4.1 Tạo và cài đặt dữ liệu kích hoạt 55](#_Toc8997980)

[VI.4.2 Bảo vệ dữ liệu kích hoạt 56](#_Toc8997981)

[VI.4.3 Các vấn đề khác của dữ liệu kích hoạt 56](#_Toc8997982)

[VI.5 Kiểm soát an ninh cho hệ thống máy tính 56](#_Toc8997983)

[VI.5.1 Các yêu cầu an ninh hệ thống máy tính 56](#_Toc8997984)

[VI.5.2 Đánh giá an ninh của hệ thống máy tính 57](#_Toc8997985)

[VI.6 Kiểm soát kỹ thuật vòng đời chứng thư số 57](#_Toc8997986)

[VI.6.1 Giám sát triển khai hệ thống 57](#_Toc8997987)

[VI.6.2 Quản lý giám sát an ninh 57](#_Toc8997988)

[VI.6.3 Giám sát an ninh vòng đời chứng thư số 57](#_Toc8997989)

[VI.7 Kiểm soát an toàn mạng 57](#_Toc8997990)

[VI.8 Cấp dấu thời gian 57](#_Toc8997991)

[VII ĐỊNH DẠNG CHỨNG THƯ SỐ, CRL VÀ OCSP 58](#_Toc8997992)

[VII.1 Hồ sơ chứng thư số 58](#_Toc8997993)

[VII.1.1 Phiên bản 58](#_Toc8997994)

[VII.1.2 Trường cơ bản 58](#_Toc8997995)

[VII.1.3 Trường mở rộng 58](#_Toc8997996)

[VII.1.4 Các thuật toán ký 59](#_Toc8997997)

[VII.1.5 Khuôn dạng tên 59](#_Toc8997998)

[VII.1.6 Giới hạn tên 59](#_Toc8997999)

[VII.1.7 Sử dụng ràng buộc mở rộng chính sách chứng thư số 59](#_Toc8998000)

[VII.1.8 Cú pháp và ngữ nghĩa của chính sách phân loại 60](#_Toc8998001)

[VII.1.9 Xử lý ngữ nghĩa của các trường mở rộng chính sách chứng thư số 60](#_Toc8998002)

[VII.2 Hồ sơ CRL 60](#_Toc8998003)

[VII.2.1 Số phiên bản của CRL 60](#_Toc8998004)

[VII.2.2 CRL và các trường mở rộng của CRL 60](#_Toc8998005)

[VII.3 Hồ sơ OCSP 60](#_Toc8998006)

[VII.3.1 Phiên bản 60](#_Toc8998007)

[VII.3.2 Trường cơ bản 61](#_Toc8998008)

[VII.3.3 Trường mở rộng 61](#_Toc8998009)

[VIII KIỂM TOÁN MỨC TUÂN THỦ VÀ CÁC ĐÁNH GIÁ KHÁC 62](#_Toc8998010)

[VIII.1 Tần suất và các tình huống kiểm toán kỹ thuật 62](#_Toc8998011)

[VIII.2 Đơn vị thực hiện kiểm toán kỹ thuật 62](#_Toc8998012)

[VIII.3 Mối quan hệ của đơn vị kiểm toán kỹ thuật với NC-CA 62](#_Toc8998013)

[VIII.4 Các nội dung kiểm toán kỹ thuật 62](#_Toc8998014)

[VIII.5 Xử lý khi phát hiện sai sót 62](#_Toc8998015)

[VIII.6 Công bố kết quả kiểm toán kỹ thuật 63](#_Toc8998016)

[IX CÁC NỘI DUNG NGHIỆP VỤ VÀ PHÁP LÝ KHÁC 63](#_Toc8998017)

[IX.1 Phí 63](#_Toc8998018)

[IX.1.1 Phí cấp phát, gia hạn, thay đổi khóa và thu hồi chứng thư số 63](#_Toc8998019)

[IX.1.2 Phí truy cập chứng thư số 63](#_Toc8998020)

[IX.1.3 Phí truy cập thông tin trạng thái thu hồi (Dịch vụ xác minh hiệu lực của chứng thư số) 63](#_Toc8998021)

[IX.1.4 Phí cho những dịch vụ khác như là thông tin về chính sách 63](#_Toc8998022)

[IX.1.5 Phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số 63](#_Toc8998023)

[IX.1.6 9.1.6. Chính sách hoàn phí 64](#_Toc8998024)

[IX.2 Trách nhiệm tài chính 64](#_Toc8998025)

[IX.2.1 Bảo hiểm 64](#_Toc8998026)

[IX.2.2 Trách nhiệm bồi thường thiệt hại cho thuê bao 64](#_Toc8998027)

[IX.2.3 Trách nhiệm bồi thường của bên khác 64](#_Toc8998028)

[IX.3 Tính bí mật của thông tin nghiệp vụ 65](#_Toc8998029)

[IX.3.1 Phạm vi các thông tin bí mật 65](#_Toc8998030)

[IX.3.2 Những thông tin ngoài phạm vi thông tin bí mật 66](#_Toc8998031)

[IX.3.3 Trách nhiệm bảo vệ các thông tin bí mật 66](#_Toc8998032)

[IX.4 Tính riêng tư của thông tin cá nhân 66](#_Toc8998033)

[IX.4.1 Kế hoạch bảo mật thông tin cá nhân 66](#_Toc8998034)

[IX.4.2 Phạm vi các thông tin cá nhân 66](#_Toc8998035)

[IX.4.3 Những thông tin ngoài phạm vi thông tin cá nhân 66](#_Toc8998036)

[IX.4.4 Trách nhiệm bảo vệ các thông tin bí mật 66](#_Toc8998037)

[IX.4.5 Thông báo và sự đồng thuận sử dụng thông tin mật 66](#_Toc8998038)

[IX.4.6 Cung cấp thông tin theo yêu cầu của cơ quan pháp luật 67](#_Toc8998039)

[IX.4.7 Các tình huống cung cấp thông tin khác 67](#_Toc8998040)

[IX.5 Quyền sở hữu trí tuệ 67](#_Toc8998041)

[IX.5.1 Quyền sở hữu những thông tin chứng thư số và thu hồi 67](#_Toc8998042)

[IX.5.2 Quyền sở hữu quy chế chứng thực 67](#_Toc8998043)

[IX.5.3 Quyền sở hữu tên 67](#_Toc8998044)

[IX.5.4 Quyền sở hữu khóa 67](#_Toc8998045)

[IX.6 Tuyên bố và cam kết 67](#_Toc8998046)

[IX.6.1 Tuyên bố và cam kết của NC-CA 67](#_Toc8998047)

[IX.6.2 Tuyên bố và cam kết của RA 68](#_Toc8998048)

[IX.6.3 Tuyên bố và cam kết của thuê bao 68](#_Toc8998049)

[IX.6.4 Tuyên bố và cam kết của người nhận 68](#_Toc8998050)

[IX.6.5 Tuyên bố và cam kết của các đối tượng khác 69](#_Toc8998051)

[IX.7 Tuyên bố về sự đảm bảo 69](#_Toc8998052)

[IX.7.1 Tuyên bố về đảm bảo hệ thống 24/7 69](#_Toc8998053)

[IX.7.2 Tuyên bố đảm bảo tuân thủ quy định phát luật và tiêu chuẩn của Bộ Thông tin và Truyền thông 69](#_Toc8998054)

[IX.8 Giới hạn về trách nhiệm 69](#_Toc8998055)

[IX.9 Bồi thường 69](#_Toc8998056)

[*IX.9.1* *Vấn đề bồi thường của thuê bao* 69](#_Toc8998057)

[*IX.9.2* *Vấn đề bồi thường của người nhận* 70](#_Toc8998058)

[IX.10 Điều khoản và sự kết thúc 70](#_Toc8998059)

[IX.10.1 Thời hạn bắt đầu có hiệu lực 70](#_Toc8998060)

[IX.10.2 Thời hạn hết hiệu lực 70](#_Toc8998061)

[IX.10.3 Ảnh hưởng của quy chế chứng thư số hết hiệu lực 70](#_Toc8998062)

[IX.11 Thông báo cho thuê bao và liên lạc với các bên có tham gia 70](#_Toc8998063)

[IX.12 Thay đổi Quy chế chứng thực 71](#_Toc8998064)

[IX.12.1 Thủ tục bổ sung 71](#_Toc8998065)

[IX.12.2 Cơ chế và thời hạn thông báo 71](#_Toc8998066)

[IX.13 Giải quyết các bất đồng , tranh chấp 71](#_Toc8998067)

[IX.14 Luật điều chỉnh 71](#_Toc8998068)

[IX.15 Tính tuân thủ với các luật pháp được áp dụng 71](#_Toc8998069)

[IX.16 Điều khoản chung 72](#_Toc8998070)

[IX.17 Điều khoản khác 72](#_Toc8998071)

[X TÀI LIỆU THAM CHIẾU 72](#_Toc8998072)

GIỚI THIỆU

CÔNG TY CỔ PHẦN HỖ TRỢ DOANH NGHIỆP VÀ ĐẦU TƯ HN là công ty hoạt động trong lĩnh vực công nghệ thông tin. Công ty có thế mạnh về tiềm lực tài chính, đội ngũ kỹ thuật giàu kinh nghiệm, có các kênh phân phối tại cả 3 miền Bắc, Trung, Nam.

công ty cổ phần hỗ trợ doanh nghiệp và đầu tư HN là một trong số những doanh nghiệp được Bộ Thông tin và Truyền thông lựa chọn cấp phép trở thành đơn vị cung cấp dịch vụ chứng thực chữ ký số. NC-CA là tên gọi của dịch vụ chứng thực chữ ký số công cộng do công ty cổ phần hỗ trợ doanh nghiệp và đầu tư HN thành lập. NC-CA có đầy đủ thẩm quyền cấp chứng thư số cho các tổ chức, doanh nghiệp, cá nhân có yêu cầu xin cấp và sử dụng chứng thư số.

NC-CA bao gồm một CA, các tổ chức đăng ký chứng thư số và các đại lý được ủy quyền. RA và các đại lý có trách nhiệm tiếp nhận và xác thực thông tin từ phía khách hàng sử dụng dịch vụ.

NC-CA dự kiến triển khai cung cấp dịch vụ chứng thực chữ ký số công cộng phục vụ khách hàng trên toàn quốc với các đối tượng chính khách hàng cá nhân, cá nhân thuộc tổ chức doanh nghiệp và tổ chức, doanh nghiệp.

## Giới thiệu về Quy chế chứng thực

Quy chế chứng thực là một tài liệu quan trọng để NC-CA phục vụ cho các hoạt động cung cấp dịch vụ chứng thực chữ ký số công cộng.

**Phạm vi của quy chế chứng thực:** Quy chế chứng thực đề cập đến các yêu cầu về quy trình, luật pháp, kỹ thuật cho quá trình xét duyệt hồ sơ, chấp nhận, tạo lập, cấp phát, quản lý, thu hồi và cấp lại chứng thư số. Các bên tham gia cấp phát và sử dụng chứng thư số phải tuân thủ các yêu cầu được đề ra trong Quy chế chứng thực này.

Quy chế chứng thực đóng vai trò quan trọng trong quá trình cung cấp dịch vụ chứng thực chữ ký số và được áp dụng cho tất cả các thành phần tham gia dịch vụ chứng thực chữ ký số NC-CA. Các thành phần tham gia dịch vụ NC-CA phải tuân thủ các yêu cầu của Quy chế chứng thực này.

Quy chế chứng thực của NC-CA được xây dựng tuân theo khuyến nghị RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework). Đồng thời Quy chế chứng thực này tuân theo sự luật pháp Việt Nam cũng như tuân theo các chính sách, quy chế, văn bản và thủ tục ban hành Bộ Thông tin và Truyền thông và các đơn vị chức năng có liên quan khác.

## Tên và định danh của tài liệu

OID của Quy chế chứng thực này là 1.3.6.1.4.1.30339.x.x.x, được xác định theo quy định của Trung tâm Chứng thực điện tử quốc gia có sử dụng dạng đánh số chuẩn của IANA như sau:

1.3.6.1.4.1.30339.[codeTypeCA].[code-CA].[codeCPS]

Trong đó, codeTypeCA được đặt là 1, code-CA được xác định khi NC-CA được Bộ Thông tin và Truyền thông cấp giấy phép hoạt động, codeCPS được gán là 3 là mã số của Quy chế chứng thực trong các tài liệu an toàn thông tin của NC-CA.

## Thành viên tham gia hệ thống PKI công cộng

### RootCA

Trung tâm Chứng thực điện tử quốc gia là đơn vị do Bộ Thông tin và Truyền thông thành lập có chức năng giúp tham mưu công tác quản lý nhà nước về lĩnh vực chứng thực chữ ký số; quản lý các tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng và chuyên dùng; cấp phát chứng thư số cho các tổ chức đăng ký cung cấp dịch vụ chứng thư số công cộng; tổ chức các hoạt động thúc đẩy việc sử dụng chữ ký số trong các ứng dụng công nghệ thông tin phục vụ phát triển kinh tế - xã hội trong phạm vi cả nước. Trung tâm Chứng thực điện tử quốc gia vận hành Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia (RootCA).

### NC-CA

Tổ chức cung cấp dịch vụ chứng thực chữ ký số (CA) công cộng là các tổ chức cung cấp dịch vụ chứng thực chữ ký số cho cơ quan, tổ chức, cá nhân sử dụng trong các hoạt động công cộng. Hoạt động của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng là hoạt động nhằm mục đích kinh doanh. RootCA quốc gia cấp chứng thư số cho các CA công cộng

NC-CA là CA công cộng cung cấp dịch vụ chứng thực chữ ký số công cộng cho cơ quan, tổ chức, cá nhân sử dụng trong các hoạt động công cộng.

**Mô hình tổ chức của NC-CA**:

NC-CA tổ chức thành các khối sau: Khối kỹ thuật, Khối kinh doanh, Khối tài chính

*Khối kinh doanh của NC-CA*. NC-CA thực hiện làm việc trực tiếp với khách hàng và sử dụng các đại lý ở cả 3 miền trên toàn quốc.

*Khối kỹ thuật* *của NC-CA* bao gồm các bộ phận: bộ phận xác minh, bộ phận phê duyệt, bộ phận cấp phát thực hiện các quy trình theo mục IV

*Khối tài chính của NC-CA* bao gồm các bộ phận liên quan đến tài chính thực hiện nhiệm vụ liên quan đến kế toán, đối soát, thu phí, …

### Thuê bao

*Thuê bao* trong hệ thống NC-CA là các cá nhân hay tổ chức sở hữu chứng thư số do NC-CA ban hành.

### Đại lý

*Đại lý* (RA) là một tổ chức được NC-CA tin cậy uỷ quyền để đảm bảo tìm kiếm khách hàng và xác minh tính đúng đắn nội dung thông tin trong chứng thư số của khách hàng. Nhiệm vụ của RA là: tìm kiếm và xác thực các thuê bao xin chứng thư số. (chú ý: NC-CA vẫn là đơn vị xác minh tính chính xác sau cùng khi cấp phát chứng thư số).

Các RA phải tuân thủ các quy định được chỉ rõ trong Quy chế chứng thực này. RA và NC-CA sẽ ký thỏa thuận quy định về quyền hạn và trách nhiệm của các bên trong việc cung cấp dịch vụ chứng thực chữ ký số.

### Bên tin tưởng

*Bên tin tưởng* là đối tượng tin tưởng chứng thư số hay một chữ ký số được cung cấp bởi NC-CA Phụ thuộc vào quy định sử dụng chứng thư số, bên tin tưởng có thể là thuê bao hoặc không là thuê bao của NC-CA.

### Các đối tượng khác

NC-CA không quản lý đối tượng nào khác ngoài thuê bao và các bên tin tưởng.

## Phương thức sử dụng chứng thư số

### Phạm vi sử dụng

Trong chứng thư số, trường KeyUsage chứa thông tin về mục đích sử dụng chứng thư số. Chứng thư số do NC-CA cấp được phân ra các loại sau đây:

* Chứng thư số cho cá nhân: Là chứng thư số cấp cho cá nhân Thuê bao sử dụng chứng thư số này trong việc ký các ứng dụng, ký email, ký các giao dịch điện tử.

Chứng thư số cho các nhân có thời hạn không quá 2 năm và không được vượt quá thời hạn của chứng thư số NC-CA.

* Chứng thư số cho cá nhân thuộc tổ chức doanh nghiệp: Là chứng thư số cấp cho cá nhân, trong chứng thư số có thông tin về tổ chức doanh nghiệp mà thuê bao trực thuộc. Thuê bao sử dụng chứng thư số này trong việc ký các ứng dụng, ký email, ký các giao dịch điện tử.

Chứng thư số cho các nhân thuộc tổ chức doanh nghiệp có thời hạn không quá 2 năm và không được vượt quá thời hạn của chứng thư số NC-CA.

* Chứng thư số cho tổ chức doanh nghiệp: Thuê bao là tổ chức doanh nghiệp. Thuê bao sử dụng chứng thư số này trong việc ký các ứng dụng, ký email, kê khai thuế điện tử, hải quan điện tử và ký các giao dịch điện tử khác.

Chứng thư số cho tổ chức doanh nghiệp có thời hạn không quá 3 năm và không được vượt quá thời hạn của chứng thư số NC-CA.

* Chứng thư số dành cho máy chủ (SSL): Thuê bao đăng ký chứng thư số này cho máy chủ có domain xác định. Đối tác thứ 3 khi truy cập vào website có thể xác thực độ tin cậy của website thông qua chứng thư số do NC-CA cấp.

Chứng thư số SSL có thời hạn không quá 2 năm và không được vượt quá thời hạn của chứng thư số NC-CA.

Khi tổ chức, doanh nghiệp đăng ký xin cấp chứng thư số cho máy chủ, thiết lập VPN, SSL/TLS thì người đại diện pháp luật của tổ chức, doanh nghiệp là người đứng ra đăng ký.

Khi thuê bao là cá nhân đăng ký xin cấp chứng thư số thì bản thân thuê bao đứng ra thực hiện đăng ký.

Chứng thư số không được sử dụng cho các mục đích ngoài các mục đích đã nêu trong trường KeyUsage và chỉ được sử dụng theo đúng phạm vi quy định trong hợp đồng giữa NC-CA và thuê bao.

Chi tiết định dạng các chứng thư số trong mục VII.1 Hồ sơ chứng thư số. Quy tắc đặt tên mục đích định danh trong trường DN, từng loại chứng thư số được định danh tại mục III.1.2 Quy tắc đặt tên

### Cấm sử dụng

Trong mọi trường hợp, cấm sử dụng chứng thư số do NC-CA cấp phát vào những mục đích đảm bảo an ninh cho lĩnh vực hạt nhân, hệ thống điều khiển vũ khí, trong lĩnh vực an ninh, quân sự, đảm bảo an ninh quốc gia, cho các hoạt động vi phạm pháp luật hoặc làm chứng thư số gốc của CA khác.

## Tổ chức quản lý chính sách

### Tổ chức quản trị tài liệu

* Công ty cổ phần hỗ trợ doanh nghiệp và đầu tư hn
* Địa chỉ: Số 439 Trương Định, Phường Tân Mai, Quận Hoàng Mai, TP Hà Nội
* Điện thoại: 02462971010
* Website: nc-ca.com.vn

### Người liên hệ

* Đường dây nóng Công ty cổ phần hỗ trợ doanh nghiệp và đầu tư hn
* Địa chỉ: Số 439 Trương Định, Phường Tân Mai, Quận Hoàng Mai, TP Hà Nội
* Điện thoại: 02462971010
* Website: nc-ca.com.vn

### Người quyết định sự phù hợp của Quy chế chứng thực chữ ký số

* Bà Trần Thị Ngà, Tổng Giám đốc Công ty cổ phần hỗ trợ doanh nghiệp và đầu tư hn
* Địa chỉ: Vị trí 6, Liền kề 8, Xa La, Hà Đông, Hà Nội
* Điện thoại: 0904.508.168

### Tổ chức phê chuẩn quy chế chứng thực

* Quy chế chứng thực của NC-CA được Bộ Thông tin và Truyền thông thông qua và được phê chuẩn bởi Tổng giám đốc công ty cổ phần hỗ trợ doanh nghiệp và đầu tư HN. Các phiên bản sửa đổi quy chế chứng thực này được thực hiện bởi Công ty cổ phần hỗ trợ doanh nghiệp và đầu tư HN và được Bộ Thông tin và Truyền thông thông qua.

### Thủ tục phê chuẩn quy chế chứng thực

* Các quá trình xem xét và phê duyệt phải đảm bảo rằng việc này CP-CPS tuân thủ RFC 3647 và các quy định có liên quan.
* Khi có sự thay đổi thông tin trong quy chế chứng thực, tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng phải thông báo bằng văn bản đến Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia và phải được sự đồng ý bằng văn bản của Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia đối với các nội dung thay đổi.. Các thay đổi, cập nhật của Quy chế chứng thực được công bố tại http://NC-CA.vn/cps
* Tất cả các phiên bản Quy chế chứng thực dựa trên đó các chứng thư số hợp lệ đang hoặc đã được cấp phát phải được lưu trữ để cung cấp cho các bên tin tưởng khi có yêu cầu. Các phiên bản của Quy chế chứng thực được công bố tại: http://NC-CA.vn/cps/version/.

## Định nghĩa và viết tắt

| **Viết tắt** | **Ý nghĩa** |
| --- | --- |
| CA | Certification Authority - Tổ chức cung cấp dịch vụ chứng thực chữ ký số |
| Chính sách bảo mật  | Văn bản quy định về thông tin được coi là bí mật và trách nhiệm giữ bí mật thông tin của các đối tượng liên quan.  |
| Chữ ký số | là một dạng chữ ký điện tử được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã không đối xứng theo đó người có được thông điệp dữ liệu ban đầu và khoá công khai của người ký có thể xác định được chính xác:a) Việc biến đổi nêu trên được tạo ra bằng đúng khoá bí mật tương ứng với khoá công khai trong cùng một cặp khóa;b) Sự toàn vẹn nội dung của thông điệp dữ liệu kể từ khi thực hiện việc biến đổi nêu trên. |
| Chứng thư số  | Một dạng chứng thư điện tử do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp |
| Chứng thư số có hiệu lực | Chứng thư số chưa hết hạn, không bị tạm dừng hoặc bị thu hồi. |
| Chuỗi chứng thư số  | Danh sách có thứ tự các chứng thư số, bắt đầu từ chứng thư số của Root CA hoặc CA (nếu đứng riêng) đến chứng thư số của người dùng cuối. Chứng thư số của đối tượng đứng trước trong danh sách được dùng để ký lên chứng thư số của đối tượng đứng sau trong danh sách.  |
| CN  | Common Name - một thuộc tính trong trường DN của chứng thư số, CN biểu diễn tên thường gọi của đối tượng là chủ thể của chứng thư số.  |
| CRL  | Certificate Revocation List - Danh sách thu hồi chứng thư số.  |
| Dịch vụ chứng thực chữ ký số | Một loại hình dịch vụ chứng thực chữ ký điện tử, do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp. Dịch vụ chứng thực chữ ký số bao gồm:a) Tạo cặp khóa bao gồm khóa công khai và khóa bí mật cho thuê bao;b) Cấp, gia hạn, và thu hồi chứng thư số của thuê bao;c) Duy trì trực tuyến cơ sở dữ liệu về chứng thư số;d) Những dịch vụ khác có liên quan theo quy định. |
| DN  | Distinguished Names – một trường trong chứng thư số, DN chưa thông tin nhận dạng đối tượng là chủ thể chứng thư số.  |
| Hệ thống mật mã không đối xứng | là hệ thống mật mã có khả năng tạo được cặp khóa bao gồm khoá bí mật và khoá công khai.  |
| KeyUsage | Mục đích sử dụng khóa |
| Khoá | một chuỗi các số nhị phân (0 và 1) dùng trong các hệ thống mật mã. |
| Khóa bí mật | một khóa trong cặp khóa thuộc hệ thống mật mã không đối xứng, được dùng để tạo chữ ký số. |
| Khóa công khai | một khóa trong cặp khóa thuộc hệ thống mật mã không đối xứng, được sử dụng để kiểm tra chữ ký số được tạo bởi khoá bí mật tương ứng trong cặp khoá |
| Ký số | việc đưa khóa bí mật vào một chương trình phần mềm để tự động tạo và gắn chữ ký số vào thông điệp dữ liệu. |
| LDAP | Lightweight Directory Access ProtocolGiao thức truy cập thư mục rút gọn |
| Người ký | thuê bao dùng đúng khoá bí mật của mình để ký số vào một thông điệp dữ liệu dưới tên của mình. |
| Người nhận (bên tin tưởng) | Tổ chức, cá nhân nhận được thông điệp dữ liệu được ký số bởi người ký, sử dụng chứng thư số của người ký đó để kiểm tra chữ ký số trong thông điệp dữ liệu nhận được và tiến hành các hoạt động, giao dịch có liên quan. |
| OCSP | Online Certificate Status Protocol - Giao thức cung cấp trạng thái chứng thư số trực tuyến |
| PKI | Public Key Infrastructure - Hạ tầng khóa công khai |
| RA | Registration Authority -Tổ chức đăng ký chứng thư số: Có chức năng giúp đỡ CA duyệt đơn đăng ký chứng thư số, đơn gia hạn chứng thư số, đơn thu hồi chứng thư số và quản lý thông tin thuê bao.  |
| Tạm dừng chứng thư số | Làm mất hiệu lực của chứng thư số một cách tạm thời từ một thời điểm xác định. |
| Thu hồi chứng thư số | Làm mất hiệu lực của chứng thư số một cách vĩnh viễn từ một thời điểm xác định. |
| Thuê bao | Tổ chức, cá nhân được cấp chứng thư số, chấp nhận chứng thư số và giữ khoá bí mật tương ứng với khoá công khai ghi trên chứng thư số được cấp đó. |
| Tổ chức cung cấp dịch vụ chứng thực chữ ký số | Tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử thực hiện hoạt động cung cấp dịch vụ chứng thực chữ ký số. |
| Token | Thiết bị lưu khóa cứng |
| Repository | Kho dữ liệu |

TRÁCH NHIỆM VỀ CÔNG BỐ VÀ LƯU TRỮ

## Kho lưu trữ

NC-CA duy trì một kho dữ liệu về các chứng thư số đã được cấp, danh sách thu hồi chứng thư số mới nhất và tất cả các phiên bản Quy chế chứng thực dựa trên đó các chứng thư số hợp lệ đã được cấp.

NC-CA duy trì kho chứa chứng thư số có hiệu lực trên nền tảng LDAP và các phiên bản chứng thư số đã được cấp phát trước đó.

Các kho dữ liệu này được xây dựng với chế độ sẵn sàng 24x7.

## Công bố thông tin về chứng thư số

NC-CA cung cấp cho người dùng phương thức kiểm tra trạng thái chứng thư số thông qua CRL và dịch vụ OCSP.

Thông tin về CRL được công bố tại <http://crl.>nc-ca.vn/nc-ca.crl

Thông tin về OCSP được công bố tại http://ocsp.NC-CA.vn/responder

Ngoài chứng thư số cấp cho thuê bao, NC-CA công bố tại trang web http://www.NC-CA.vn/download/ các thông tin sau:

* Chứng thư số gốc của NC-CA
* Biểu mẫu đăng ký cấp chứng thư số và thoả thuận với người sử dụng
* Các thông tin về NC-CA
* Quy trình cấp phát, quản lý và sử dụng chứng thư số

## Thông tin về tần suất công bố

NC-CA công bố thông tin với tần số sau đây:

* Chứng thư số được công bố theo thời gian thực.
* CRL được công bố hàng ngày.
* Quy chế chứng thực được công bố ngay khi có hiệu lực. Các phiên bản của Quy chế chứng thực được cung cấp theo yêu cầu.
* Các thông tin khác: theo yêu cầu.

## Kiểm soát truy cập vào kho lưu trữ

Truy cập đến các thông tin nêu trong Kho lưu trữ mục II.1và Công bố thông tin chứng thư số với mục đích đọc không bị giới hạn. NC-CA không sử dụng biện pháp kỹ thuật để giới hạn truy cập với mục đích lấy chứng thư số và kiểm tra thông tin trạng thái của chứng thư số.

NC-CA sử dụng biện pháp kỹ thuật để hạn chế những hành động thêm, xoá hay sửa kho lưu trữ. Các hành động truy cập trái phép sẽ bị xử lý theo quy định của công ty và pháp luật.

ĐỊNH DANH VÀ XÁC THỰC

## Đặt tên

 Phân loại

Chứng thư số NC-CA được phân loại như sau:

* Chứng thư số tổ chức
* Chứng thư số cá nhân
* Chứng thư số SSL

 Quy định đặt tên

Tên của chứng thư số NC-CA cấp phát được dùng để phân biệt với các chứng thư số khác theo chuẩn X.509 v3 trong trường ‘Issuer’ và ‘Subject’.

Nguyên tắc đặt tên với nghĩa dễ hiểu cho phép nhận dạng được cá nhân, tổ chức, doanh nghiệp sở hữu chứng thư số đó. Tên có ý nghĩa của thuê bao trong chứng thư số là tên cho phép xác định được đối tượng sở hữu của chứng thư số. Khi có yêu cầu của pháp luật, tên trong một chứng thư số được cấp phát phải chỉ ra đúng thuê bao mà tên này được gán.

Các thuộc tính trong DN của chứng thư số do NC-CA cấp cho thuê bao là doanh nghiệp được mô tả như sau:

|  |  |
| --- | --- |
| **Thuộc tính** | **Giá trị** |
| Tổ chức (O)  | Tên tổ chức mà thuê bao sở hữu chứng thư số |
| Bộ phận tổ chức (OU)  | Bộ phận thuộc tổ chức (O) mà thuê bao sở hữu chứng thư số trực thuộc.  |
| Quận, huyện (L) | Địa chỉ quận/ huyện của thuê bao |
| Tỉnh, thành phố (ST) | Địa chỉ tỉnh, thành phố của thuê bao |
| Quốc gia (C) | Tên quốc gia của thuê bao |
| Mã định danh của thuê bao - UID | Mã số Thuế: Đối với khách hàng là tổ chức, doanh nghiệp hoặc Mã đơn vị hoặc Mã ngân sách hoặc Mã định danh thỏa thuận giữa khách hàng và NC-CA |
| Tên thường gọi (CN)  | Tên của tổ chức, doanh nghiệp (Theo như quyết định thành lập hay giấy đăng ký kinh doanh, và một số giấy tờ khác) |
| Địa chỉ email (E)  | Địa chỉ email giao dịch của thuê bao sở hữu chứng thư số |

Các thuộc tính trong DN của chứng thư số do NC-CA cấp cho thuê bao là cá nhân thuộc doanh nghiệp được mô tả như sau:

|  |  |
| --- | --- |
| **Thuộc tính** | **Giá trị** |
| Tổ chức (O)  | Tên tổ chức mà thuê bao sở hữu chứng thư số |
| Bộ phận tổ chức (OU)  | Bộ phận thuộc tổ chức (O) mà thuê bao sở hữu chứng thư số trực thuộc.  |
| Quận, huyện (L) | Địa chỉ quận/ huyện của thuê bao |
| Tỉnh, thành phố (ST) | Địa chỉ tỉnh, thành phố của thuê bao |
| Quốc gia (C) | Tên quốc gia của thuê bao |
| Mã định danh của thuê bao - UID | CMND: Đối với khách hàng cá nhân thuộc tổ chức, doanh nghiệp. |
| Tên thường gọi (CN)  | Tên thuê bao sở hữu chứng thư số (Theo như giấy giới thiệu của tổ chức doanh nghiệp, hợp đồng lao động và một số giấy tờ khác) |
| Địa chỉ email (E)  | Địa chỉ email giao dịch của thuê bao sở hữu chứng thư số |

Các thuộc tính trong DN của chứng thư số do NC-CA cấp cho thuê bao là cá nhân được mô tả như sau:

|  |  |
| --- | --- |
| **Thuộc tính** | **Giá trị** |
| Quận, huyện (L) | Địa chỉ quận/ huyện của thuê bao |
| Tỉnh, thành phố (ST) | Địa chỉ tỉnh, thành phố của thuê bao |
| Quốc gia (C) | Tên quốc gia của thuê bao |
| Mã định danh của thuê bao - UID | CMND: Đối với khách hàng cá nhân hoặc Mã nhân viên hoặc Mã định danh thỏa thuận của khách hàng với NC-CA |
| Tên thường gọi (CN)  | Tên thuê bao sở hữu chứng thư số (Theo như giấy CMND hoặc một số giấy tờ khác) |
| Địa chỉ email (E)  | Địa chỉ email giao dịch của thuê bao sở hữu chứng thư số |

Chứng thư số SSL có các thuộc tính trong DN cấp cho thuê bao như sau:

|  |  |
| --- | --- |
| **Thuộc tính** | **Giá trị** |
| Tổ chức (O)  | Tên tổ chức mà thuê bao sở hữu chứng thư số (nếu có) |
| Bộ phận tổ chức (OU)  | Bộ phận thuộc tổ chức (O) mà thuê bao sở hữu chứng thư số trực thuộc. (nếu có) |
| Quận, huyện (L) | Địa chỉ quận/ huyện của thuê bao |
| Tỉnh, thành phố (ST) | Địa chỉ tỉnh, thành phố của thuê bao |
| Quốc gia (C) | Tên quốc gia của thuê bao |
| Tên thường gọi (CN)  | Tên miền (Theo như giấy tờ chứng minh tên miền thuê bao sở hữu) |
| Địa chỉ email (E)  | Địa chỉ email giao dịch của thuê bao sở hữu chứng thư số |

DN trong chứng thư số có một thành phần là CN (viết tắt của Common Name - tên thường gọi) và đặt trong trường ‘Subject name’ của thuê bao. CN trong chứng thư số của thuê bao của là tên cá nhân, tổ chức, doanh nghiệp hoặc tên miền, tên thiết bị,….CN được kiểm tra, xác thực trong quá trình cấp chứng thư số.

 Biệt hiệu hay nặc danh

Chứng thư số của các thuê bao không được sử dụng biệt hiệu hoặc nặc danh cho tên. Việc sử dụng biệt hiệu hoặc nặc danh cho tên trong chứng thư số chỉ được chấp nhận khi có yêu cầu của pháp luật và cần có giải trình với NC-CA để xem xét.

 Tính duy nhất của tên

Tính duy nhất của tên bao gồm mã định danh thuê bao và số hiệu chứng thư

 Chấp nhận, xác thực và vai trò của nhãn hiệu đăng ký (TradeMarks)

Thuê bao xin cấp chứng thư số không được sử dụng những tên vi phạm quyền sở hữu trí tuệ. Nếu có sự tranh chấp xảy ra về sở hữu thì NC-CA có quyền thu hồi, chứng thư số hay loại bỏ đơn xin cấp chứng thư số mà không phải chịu trách nhiệm pháp lý.

## Xác minh khi cấp chứng thư số lần đầu

Khi cần thiết, người có thẩm quyền của NC-CA có thể yêu cầu gặp trực tiếp người đăng ký thuê bao hay đại diện có thẩm quyền của tổ chức, doanh nghiệp đăng ký thuê bao chứng thư số khi người đại diện này đến xin cấp chứng thư số.

 Phương pháp chứng minh sở hữu khóa riêng

Thuê bao phải chứng minh được thuê bao thực sự sở hữu khóa riêng tương ứng với khóa công khai được đề nghị cấp chứng thư số.

Các phương pháp chứng minh thuê bao thực sự sở hữu khóa riêng:

* Tệp tin đề nghị cấp chứng thư số mã hóa theo chuẩn PKCS #10 sinh từ PKI Smartcard, PKI Token, PKI Virtual Token đạt chuẩn FIPS 140-2 Level 2 trở lên, hoặc tương đương do thuê bao thực hiện;
* Hoặc thuê bao ủy quyền cho NC-CA, NC-CA sinh khóa theo ủy quyền của thuê bao sử dụng PKI Smartcard, PKI Token, PKI Virtual Token đạt chuẩn FIPS 140-2 Level 2 trở lên. Theo quy trình, NC-CA đảm bảo quyền sở hữu khóa riêng của thuê bao và bàn giao an toàn tránh các rủi ro trong quá trình giao nhận.

 Kiểm tra nhận dạng thông tin của tổ chức doanh nghiệp

Kiểm tra nhận dạng của người đại diện theo pháp luật của tổ chức doanh nghiệp dựa trên các thủ tục thông thường để nhận dạng.

Người đại diện của tổ chức, doanh nghiệp khi đến giao dịch cần xuất trình:

* Kiểm tra tính hợp lệ của đơn đề nghị cấp chứng thư số.
* Giấy giới thiệu, uỷ quyền của tổ chức, doanh nghiệp
* Chứng minh thư nhân dân của người đại diện.
* Các giấy tờ liên quan như quyết định thành lập, giấy phép đăng ký kinh doanh, mã số thuế.
* Các thông tin khác theo quy định của pháp luật (nếu cần).

Các thông tin cần thiết sẽ được ghi lại bởi hệ thống của NC-CA.

 Xác thực nhận dạng thông tin của cá nhân

Nhận dạng của cá nhân và thông tin liên quan được cung cấp bởi đối tượng đăng ký chứng thư số sẽ được xác minh theo thủ tục được NC-CA quy định, bao gồm ít nhất các bước sau:

* Kiểm tra tính hợp lệ của đơn đề nghị cấp chứng thư số.
* Kiểm tra thông tin đăng ký của cá nhân thuê bao với thông tin như CMND.
* Đối với khách hàng đăng ký chứng thư cá nhân thuộc tổ chức doanh nghiệp thì kiểm tra giấy giới thiệu, các giấy tờ chứng minh khách hàng đang công tác tại tổ chức doanh nghiệp.
* Trong trường hợp cần thiết, xác thực thông tin cá nhân dựa vào sự hiện diện và kiểm tra các giấy tờ tùy thân như hộ chiếu, chứng minh thư của cá nhân người đăng ký.

Xác thực nhận dạng bằng cách so sánh thông tin đăng ký với thông tin chứa trong cơ sở dữ của đối tác đáng tin cậy.

 Xác thực danh tính tên miền hoặc thiết bị

Khi có một yêu cầu đăng ký chứng thư số cho tên miền hoặc thiết bị, nhận dạng của thuê bao được kiểm tra trên các hệ thống đang hoạt động và xác minh về quyền sở hữu của tổ chức với domain và email đó.

Thông tin định danh sau đây của tên miền hoặc thiết bị bắt buộc phải được xác minh và ghi lại:

* Giấy giới thiệu, uỷ quyền của tổ chức, doanh nghiệp (nếu ủy quyền)
* Chứng minh thư nhân dân của người được ủy quyền.
* Các giấy tờ liên quan như quyết định thành lập, giấy phép đăng ký kinh doanh, mã số thuế.
* Giấy tờ chứng minh quyền sở hữu tên miền, thiết bị
* Nếu tổ chức doanh nghiệp ủy quyền cho một cá nhân đứng tên đăng ký chứng thư số cho mình hay cho thiết bị thì giấy giới thiệu, ủy quyền phải được lưu lại.

 Trường hơp thuê bao tự tạo cặp khóa

NC-CA chỉ cho phép thuê bao đăng ký chứng thư số cho máy chủ SSL được tự tạo cặp khóa. Thuê bao yêu cầu xin cấp chứng thư số phải chứng minh quyền sở hữu khóa bí mật tương ứng với khóa công khai trong chứng thư số. Việc này được thực hiện thông qua việc kiểm tra chữ ký số trên Yêu cầu cấp chứng thư số (Certificate request). Thuê bao phải chứng minh việc sinh khóa đảm bảo bí mật, an toàn, đúng theo quy trình và thuê bao phải chịu trách nhiệm về việc bảo mật, lộ cặp khóa của mình.

 Thông tin không xác minh

NC-CA không xác minh những thông tin của thuê bao mà không liên quan đến quy trình quản lý vòng đời chứng thư số. NC-CA không chịu trách nhiệm về những thông tin này.

 Xác minh ủy quyền

Trong trường hợp thông tin có ủy quyền, NC-CA cần xác minh tính hiệu lực của ủy quyền.

 Tiêu chuẩn tích hợp

NC-CA áp dụng theo danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số liên quan đến chuẩn kỹ thuật tích hợp.

## Định danh và xác thực khi yêu cầu thay đổi khóa

Trước khi chứng thư số hết hạn, nếu có nhu cầu thuê bao cần phải đăng ký để có được một chứng thư số mới. Hệ thống cho phép gia hạn (renewal) theo nghĩa sinh một cặp khóa mới thay thế cặp khóa trong chứng thư số đã hết hạn.

 Định danh và xác thực khi yêu cầu thay đổi khóa

NC-CA chỉ cho phép tạo khóa lại trong thời gian có hiệu lực của chứng thư số, với thông tin giữ nguyên và cặp khóa được tạo mới.

Ngay khi thuê bao nghi ngờ khóa bí mật ko an toàn

Có Đơn đề nghị tạo khóa lại của thuê bao.

Đối với thuê bao cá nhân: Thuê bao phải xuất trình CMND

Đối với thuê bao là tổ chức, doanh nghiệp: Có Giấy ủy quyền cho đại diện, Giấy CMND của người được ủy quyền.

Chứng minh quyền sở hữu khóa bí mật: thuê bao sử dụng chứng thư số và khóa bí mật của mình để chứng minh là có sở hữu khóa này.

NC-CA sẽ liên lạc với thuê bao thông qua điện thoại, e-mail, thư tín hay các phương tiện khác để khẳng định lại chính thuê bao đã yêu cầu tạo khóa lại.

 Nhận dạng và xác thực yêu cầu gia hạn chứng thư số

NC-CA chỉ cho phép kéo dài thời gian có hiệu lực của chứng thư số, với thông tin giữ nguyên và cặp khóa được tạo mới.

Thời hạn xin làm mới khóa của thuê bao: từ [90] ngày trước khi chứng thư số hết hạn cho tới [30] ngày sau thời điểm chứng thư số hết hạn. Sau 30 ngày hết hạn chứng thư số, yêu cầu làm mới chứng thư số sẽ không được chấp nhận, thuê bao ngoài phải thực hiện lại các bước như đăng ký mới.

Có Đơn đề nghị gia hạn chứng thư số của thuê bao

Có Giấy ủy quyền cho đại diện đến giao dịch gia hạn chứng thư số của tổ chức, doanh nghiệp là thuê bao ngoài.

Chứng minh quyền sở hữu khóa bí mật: thuê bao sử dụng chứng thư số và khóa bí mật của mình để chứng minh là có sở hữu khóa này.

NC-CA sẽ liên lạc với thuê bao thông qua điện thoại, e-mail, thư tín hay các phương tiện khác để khẳng định lại chính thuê bao đã yêu cầu làm mới chứng thư số. Các đặc trưng (DN) trong chứng thư số chứa tên miền, hoặc sự tồn tại thực sự của tổ chức có thể được kiểm tra bổ sung dựa vào nhà cung cấp tên miền hoặc các đơn vị hữu quan như Cơ quan thuế, Sở Kế hoạch Đầu tư.

## Định danh và xác thực khi yêu cầu thu hồi chứng thư số

Việc định danh và xác thực khi yêu cầu thu hồi chứng thư số phải có đơn xin thu hồi chứng thư số nêu rõ lý do.

NC-CA liên lạc với thuê bao thông qua điện thoại, email, thư tín hay các phương tiện khác (đã được lưu lại khi khách hàng đăng ký chứng thư số)để khẳng định lại chính thuê bao đã yêu cầu thu hồi chứng thư số.

YÊU CẦU VẬN HÀNH VỀ VÒNG ĐỜI CHỨNG THƯ SỐ

##  Đăng ký chứng thư số

 Các đối tượng có thể xin cấp chứng thư số

Các đối tượng sau có thể gửi đăng ký cấp chứng thư số:

* Cá nhân.
* Cá nhân thuộc các tổ chức, doanh nghiệp
* Tổ chức, doanh nghiệp đang hoạt động hợp pháp.

 Hồ sơ xin cấp chứng thư bao gồm:

* Đơn xin cấp chứng thư theo mẫu
* Đối với Khách hàng là cá nhân: Chứng minh nhân dân hoặc căn cước công dân hoặc hộ chiếu;
* Đối với Khách hàng là cá nhân thuộc tổ chức doanh nghiệp: Giấy CMND, hộ chiếu, giấy giới thiệu của tổ chức doanh nghiệp, hợp đồng lao động.
* Đối với Khách hàng là tổ chức doanh nghiệp: Quyết định thành lập hoặc quyết định quy định về chức năng, nhiệm vụ, quyền hạn, cơ cấu tổ chức hoặc giấy chứng nhận đăng ký doanh nghiệp hoặc giấy chứng nhận đầu tư; chứng minh nhân dân, hoặc căn cước công dân hoặc hộ chiếu của người đại diện theo pháp luật của tổ chức.
* Đối với khách hàng đăng ký chứng thư số cho máy chủ SSL: Giấy tờ chứng minh sở hữu tên miền, (nếu khách hàng là tổ chức doanh nghiệp thì cần Giấy CMND của người đại diện tổ chức doanh nghiệp, Giấy đăng ký mã số thuế, giấy tờ ủy quyền cho người đi đăng ký.)
* Cá nhân, tổ chức có quyền lựa chọn nộp bản sao từ sổ gốc, bản sao có chứng thực hoặc nộp bản sao xuất trình kèm bản chính để đối chiếu.

 Đăng ký cấp chứng thư số và trách nhiệm của các bên

Thủ tục cấp phát chứng thư số

**Bước 1:** Gửi hồ sơ xin cấp phát chứng thư số

Thuê bao làm hồ sơ theo mẫu, nộp các giấy tờ hợp lệ liên quan để xin cấp chứng thư số.

Thuê bao có thể nộp hồ sơ thẳng tới NC-CA hoặc đại lý được ủy quyền của NC-CA (hay còn gọi là RA của NC-CA)

**Bước 2**: Trường hợp thuê bao liên hệ với đại lý, đại lý tiếp nhận, xác minh sự hợp lệ của hồ sơ.

Sau khi nhận đủ hồ sơ hợp lệ, đại lý thông báo với thuê bao thời gian thông thường sẽ trả kết quả, ký kết hợp đồng và bàn giao chứng thư số.

Các đại lý có trách nhiệm tư vấn cho khách hàng hoàn thiện hồ sơ xin cấp chứng thư số đầy đủ, hợp lệ. Nhân viên được giao nhiệm vụ tại các đại lý tiếp nhận hồ sơ xin cấp chứng thư số, kiểm tra và xác minh định danh:

* Kiểm tra việc khai báo đầy đủ thông tin theo yêu cầu, thực hiện xác minh định danh theo quy định của NC-CA. Nếu thông tin không đúng và không đầy đủ, thông báo cho thuê bao để cập nhật, bổ xung hoặc thông báo từ chối cấp chứng thư số. Nếu đúng thì thông báo và hẹn thời gian để thuê bao nhận chứng thư số.
* Chuyển hồ sơ khách hàng tới NC-CA.

**Bước 3**: Nhập thông tin yêu cầu xin cấp chứng thư số

NC-CA nhận được thông tin thuê bao từ đại lý hoặc trực tiếp thuê bao.

Trường hợp thuê bao liên hệ với đại lý, đại lý thực hiện bước 2, gửi hồ sơ lên NC-CA.

Trường hợp thuê bao liên hệ với NC-CA, NC-CA sẽ nhận hồ sơ.

Khi nhận được thông tin thuê bao từ đại lý hoặc trực tiếp thuê bao, NC-CA (bộ phận nhận) xác minh sơ bộ các hồ sơ xin cấp chứng thư số. Nếu hồ sơ đầy đủ giấy tờ theo qui định, Bộ phận nhận của NC-CA nhập thông tin vào hệ thống và chuyển tới bộ phận xác minh.

Nếu hồ sơ không đầy đủ theo quy định, NC-CA thông báo lại cho đại lý hoặc thuê bao.

**Bước 4:** Thực hiện xác minh

Bộ phận CA xác minh thực hiện xác minh chi tiết thông tin để phê duyệt cấp phát chứng thư số (Approve) chứng thư số cho các thuê bao được nhập. Đây là bước xác minh chính xác trong quá trình cấp phát để đảm bảo chứng thư số sinh ra đúng đắn. Bộ phận xác minh thực hiện:

* Đối chiếu thông tin yêu cầu cấp phát chứng thư số với các thông tin trong hồ sơ của thuê bao. Đồng thời bộ phận xác minh đối chiếu với các nguồn thông tin khác trên dữ liệu điện tử quốc gia. Ngoài ra, bộ phận xác minh có thể xác minh qua kênh trực tiếp hoặc gián tiếp khác nếu thấy cần thiết. Khi thấy thông tin là đúng và đầy đủ theo quy định, sẽ thực hiện phê duyệt cấp phát chứng thư số (approve) và chuyển tới bộ phận cấp phát chứng thư.
* Đảm bảo Cặp khóa được sinh trong thiết bị chuyên dụng đáp ứng chuẩn

**Bước 5**: Thực hiện cấp phát chứng thư số

Bộ phận cấp phát chứng thư số cho các thuê bao thự hiện:

* Thực hiện thao tác cấp phát chứng thư số
* Sau khi cấp phát xong, ký vào hồ sơ và chuyển lại cho bộ phận xác minh để thực hiện kiểm tra việc cấp phát (nếu cần)
* Dữ liệu liên quan đến Hồ sơ thuê bao xin cấpchứng thư số sẽ được hệ thống lưu trữ có bảo mật theo quy định.

**Bước 6:** Thông báo chứng thư số được phê duyệt

Cặp khóa của thuê bao được sinh trực tiếp trong các thiết bị chuyên dụng. Đồng thời chứng thư số được đưa vào trong thiết bị.

Hệ thống NC-CA sẽ gửi một thư điện tử (Email) vào thư điện tử của Thuê bao (đã đăng ký trong hồ sơ), hoặc thông báo qua điện thoại về việc hoàn tất cấp phát chứng thư số.

**Bước 7:** Xác nhận đã nhận chứng thư số

Thuê bao ký vào bản xác nhận đã nhận được chứng thư số, hoàn tất các thủ tục theo như hợp đồng cung cấp dịch vụ chứng thực chữ ký số.

**Bước 8**: Công bố trạng thái chứng thư số

Hệ thống NC-CA sẽ công bố trạng thái chứng thư số ngay sau khi có thông tin thuê bao xác minh tính chính xác của chứng thư số công khai trạng thái chứng thư số thông qua dịch vụ web, CRL và OCSP theo quy định.

Thuê bao và Bên tin tưởng có thể tải CRL hoặc dùng dịch vụ OCSP để kiểm tra trạng thái của chứng thư số hoặc dùng cho các ứng dụng khác thông qua máy chủ Web.

##  Xử lý hồ sơ đăng ký chứng thư số

 Nhận dạng và xác thực

NC-CA và RA thực hiện nhận dạng và xác thực mọi thông tin trong yêu cầu cấp chứng thư số. NC-CA thực hiện nhận dạng và xác thực cuối cùng trước khi cấp chứng thư số.

Nội dung nhận dạng và xác thực:

- Hồ sơ thuê bao đầy đủ hợp lệ

- Thông tin trong hồ sơ đề nghị cấp chứng thư số của thuê bao là chính xác;

- Khóa công khai trên chứng thư số sẽ được cấp là duy nhất và cùng cặp với khóa bí mật của tổ chức, cá nhân đề nghị cấp chứng thư số.

 Duyệt đăng ký cấp chứng thư số

NC-CA sẽ chấp nhận đơn đăng ký chứng thư số nếu các điều kiện sau đây thỏa mãn:

* Mọi thông tin cần xác thực được nhận dạng và xác thực đúng.
* Thuê bao nộp đầy đủ các khoản phí theo quy định.

NC-CA không chấp nhận đơn đăng ký chứng thư số nếu:

* Một trong các thông tin cần xác thực là không chính xác.
* Thuê bao không cung cấp đầy đủ tài liệu xác minh thông tin đã kê khai trong đơn đăng ký.
* Đối tượng không thuộc diện được cấp chứng thư số.

 Thời gian xử lý đăng ký cấp chứng thư số

Thời gian xử lý một yêu cầu cấp chứng thư số tối đa là 5 ngày làm việc.

##  Cấp chứng thư số

 Thuê bao đăng ký cấp chứng thư số

Thuê bao có nhu cầu sử dụng chứng thư số liên hệ với đại lý hoặc NC-CA để được tư vấn sau đó hoàn thiện hồ sơ theo yêu cầu và gửi tới đại lý hoặc NC-CA.

 NC-CA tạo chứng thư số

Chứng thư số được cấp phát sau khi NC-CA chấp nhận đơn xin cấp chứng thư số.

NC-CA tạo cho thuê bao một chứng thư số dựa vào những thông tin trong đơn xin cấp chứng thư số và yêu cầu cấp chứng thư số.

 Thông báo cho thuê bao khi đã tạo xong chứng thư số

NC-CA gửi email hoặc điện thoại, fax thông báo cho thuê bao về việc yêu cầu cấp chứng thư số của thuê bao đã được phê duyệt.

Khi bàn giao chứng thư số chứa trong Token/Smartcard, thuê bao có trách nhiệm ký vào bản xác nhận đã nhận đầy đủ chứng thư số của mình và gửi lại NC-CA.

Nếu thông tin trong chứng thư số không phù hợp, người dùng thông báo lại cho đại lý hoặc NC-CA để được xử lý.

Thời gian thông báo cho thuê bao sau khi tạo xong chứng thư số tối đa 24h.

##  Chấp nhận chứng thư số

 Tổ chức bàn giao và xác nhận

NC-CA thực hiện bàn giao chứng thư số và yêu cầu thuê bao kiểm tra, xác nhận tính chính xác của thông tin thuê bao trên chứng thư số do NC-CA cấp theo đề nghị của thuê bao.

Thuê bao xác nhận tính chính xác của thông tin bằng email cấp trong chứng thư số và ký nhận biên bản bàn giao token.

NC-CA sẽ tiến hành bàn giao mã PIN qua email của thuê bao sau khi thuê bao đã nhận token và có xác nhận email hợp lệ.

Thuê bao phải xác nhận trước khi NC-CA công bố chứng thư số của thuê bao trên cơ sở dữ liệu trực tuyến về chứng thư số của NC-CA.

 Công bố chứng thư số

Chứng thư số được coi là chính thức chấp nhận khi được NC-CA công bố trên website, kho dữ liệu chứng thư số. NC-CA công bố chứng thư số của thuê bao tại trang web <http://www.nc-ca.vn> trong vòng 24h ngay khi nhận được xác nhận của thuê bao về tính chính xác của thông tin.

 Thông báo sự ban hành chứng thư số

NC-CA sẽ thông báo về việc cấp chứng thư số các thuê bao khác nếu cần thiết.

##  Sử dụng chứng thư số và cặp khóa

 Sử dụng khóa bí mật và chứng thư số

Thuê bao được sử dụng chứng thư số và khóa bí mật tương ứng nếu chứng thư số được coi là chấp nhận.

Chứng thư số cần được sử dụng hợp pháp, theo quy định và thỏa thuận với NC-CA, với các điều khoản của chính sách chứng thư số và quy chế chứng thực của NC-CA.

Mục đích sử dụng chứng thư số phải nhất quán với phạm vi sử dụng được phép và có ghi tại trường KeyUsage trong chứng thư số.

 Sử dụng khóa công khai và chứng thư số

Người nhận cần dựa vào các thông tin sau để đánh giá sự tin cậy của chứng thư số:

* Mục đích sử dụng của chứng thư số thể hiện trên chứng thư số (trong trường KeyUsage). Chi tiết của các mục đích sử dụng này được thể hiện trong các tài liệu thỏa thuận thuê bao, quy chế chứng thực, chính sách chứng thư số và các tài liệu liên quan đến các hoạt động nghiệp vụ có sử dụng dịch vụ chứng thực chữ ký số của NC-CA.
* Trạng thái của chứng thư số.

##  Gia hạn chứng thư số

Gia hạn chứng thư số là việc ban hành một chứng thư số mới và và một cặp khoá mới cho thuê bao sau thời hạn sử dụng chứng thư số, mọi thông tin khác trong chứng thư số đều không thay đổi. Thủ tục gia hạn chứng thư số tương tự thủ tục cấp mới chứng thư số và mức phí gia hạn sẽ thấp hơn mức phí cấp mới.

**Bước 1:** Gửi hồ sơ xin gia hạn

Thuê bao làm hồ sơ theo mẫu để xin gia hạn chứng thư. Thuê bao có thể liên hệ với đại lý hoặc liên hệ trực tiếp NC-CA

**Bước 2**: Trường hợp thuê bao liên hệ với đại lý, đại lý tiếp nhận, xác minh sự hợp lệ của hồ sơ.

Sau khi nhận đủ hồ sơ hợp lệ, đại lý thông báo với thuê bao thời gian thông thường sẽ trả kết quả, ký kết hợp đồng và bàn giao chứng thư số.

Các đại lý có trách nhiệm tư vấn cho khách hàng hoàn thiện hồ sơ xin cấp chứng thư số đầy đủ, hợp lệ. Nhân viên được giao nhiệm vụ tại các đại lý tiếp nhận hồ sơ xin cấp chứng thư số, kiểm tra và xác minh định danh:

* Kiểm tra việc khai báo đầy đủ thông tin theo yêu cầu, thực hiện xác minh định danh theo quy định của NC-CA. Nếu thông tin không đúng và không đầy đủ, thông báo cho thuê bao để cập nhật, bổ xung hoặc thông báo từ chối cấp chứng thư số. Nếu đúng thì thông báo và hẹn thời gian để thuê bao nhận chứng thư số.
* Chuyển hồ sơ khách hàng tới NC-CA.

**Bước 3:** Nhập thông tin gia hạn chứng thư số

NC-CA nhận được thông tin thuê bao từ đại lý hoặc trực tiếp thuê bao.

Trường hợp thuê bao liên hệ với đại lý, đại lý thực hiện bước 2, gửi hồ sơ xin gia hạn lên NC-CA.

Trường hợp thuê bao liên hệ với NC-CA, NC-CA sẽ nhận hồ sơ.

Khi nhận được thông tin thuê bao từ đại lý hoặc trực tiếp thuê bao, NC-CA (bộ phận nhận) xác minh sơ bộ các hồ sơ xin gia hạn chứng thư số. Nếu hồ sơ đầy đủ giấy tờ theo qui định, Bộ phận nhận của NC-CA nhập thông tin vào hệ thống và chuyển tới bộ phận xác minh.

Nếu hồ sơ không đầy đủ theo quy định, NC-CA thông báo lại cho đại lý hoặc thuê bao.

**Bước 4**: Xác minh gia hạn chứng thư số

Bộ phận NC-CA thực hiện xác minh:

* Đối chiếu thông tin yêu cầu gia hạn chứng thư số với các thông tin trong hồ sơ của thuê bao. Đồng thời bộ phận xác minh đối chiếu với các nguồn thông tin khác trên dữ liệu điện tử quốc gia. Ngoài ra, bộ phận xác minh có thể xác minh qua kênh trực tiếp hoặc gián tiếp khác nếu thấy cần thiết. Khi thấy thông tin là đúng và đầy đủ theo quy định, sẽ thực hiện phê duyệt cấp phát chứng thư số (approve) và chuyển tới bộ phận cấp phát chứng thư.
* Đảm bảo cặp khóa được sinh trong thiết bị chuyên dụng đáp ứng chuẩn
* Đảm bảo dữ liệu liên quan đến Hồ sơ thuê bao xin gia hạn chứng thư số sẽ được hệ thống lưu trữ có bảo mật theo quy định.

**Bước 4**: Thực hiện cấp phát chứng thư số

Bộ phận cấp phát chứng thư số cho các thuê bao thực hiện:

* Thực hiện thao tác cấp phát chứng thư số
* Sau khi cấp phát xong, ký vào hồ sơ và chuyển lại cho bộ phận xác minh để thực hiện kiểm tra việc cấp phát (nếu cần)
* Dữ liệu liên quan đến Hồ sơ thuê bao xin cấpchứng thư số sẽ được hệ thống lưu trữ có bảo mật theo quy định.

**Bước 5**: Thông báo chứng thư số được phê duyệt

NC-CA sẽ gửi thư điện tử (Email) tới thư điện tử của Thuê bao (đã đăng ký trong hồ sơ), hoặc điện thoại, fax tới thuê bao với nội dung thư thông báo hoàn thành việc gia hạn và hẹn thời gian bàn giao chứng thư số.

**Bước 6**: Xác nhận đã nhận chứng thư số

Thuê bao ký vào bản xác nhận đã nhận được chứng thư số, và gửi lại NC-CA (hoặc đại lý và đại lý gửi lại NC-CA)

**Bước 7**: Công bố trạng thái thư số

Hệ thống NC-CA sẽ công bố trạng thái chứng thư số ngay sau khi nhận được xác nhận của khách hàng về tính chính xác của chứng thư số được gia hạn và công khai trạng thái chứng thư số thông qua dịch vụ web, CRLs và OCSP theo quy định.

Thuê bao và Bên tin tưởng có thể tải CRLs để kiểm tra trạng thái của chứng thư số, hoặc sử dụng dịch vụ OCSP để kiểm tra trạng thái chứng thư số. Thuê bao có thể dùng cho các ứng dụng khác thông qua máy chủ Web.

**Bước 8**: Công bố trạng thái chứng thư số

Hệ thống NC-CA sẽ công bố công khai chứng thư số thông qua kho lưu trữ LDAP.

Thuê bao và Bên tin tưởng có thể tải chứng thư số về sử dụng thông qua thông qua giao diện web hoặc LDAP.

Các tình huống gia hạn chứng thư số

Trước khi hết hạn, để đảm bảo hoạt động ký số, thuê bao cần phải gia hạn chứng thư số.

Một chứng thư số có thể được gia hạn sau khi hết hạn với điều kiện các thông tin ghi trong chứng thư số cũ không thay đổi.

Thời gian gia hạn của thuê bao không quá 1 năm cho mỗi lần gia hạn.

Đối tượng có thể yêu cầu gia hạn chứng thư số

Chỉ đối tượng đăng ký chứng thư số mới có quyền yêu cầu gia hạn chứng thư số đó.

Xử lý yêu cầu gia hạn chứng thư số

NC-CA tiến hành xác minh yêu cầu gia hạn chứng thư số như trong phần cấp chứng thư số mới

Chỉ trong trường hợp thông tin thuê bao không thay đổi, chứng thư số mới có thể được gia hạn.

Thông báo sự tạo chứng thư số mới cho thuê bao

Thông báo về việc ban hành chứng thư số mới khi gia hạn chứng thư số cũng giống như thông báo khi chứng thư số được cấp mới.

Bàn giao và xác nhận với thuê bao

NC-CA thực hiện bàn giao chứng thư số và yêu cầu thuê bao kiểm tra, xác nhận tính chính xác của thông tin thuê bao trên chứng thư số do NC-CA gia hạn theo đề nghị của thuê bao.

Thuê bao phải xác nhận trước khi NC-CA công bố chứng thư số của thuê bao trên cơ sở dữ liệu trực tuyến danh bạ về chứng thư số của NC-CA.

Công bố chứng thư số mới được gia hạn

Tương tự phần IV.4.

Thông báo tạo chứng thư số mới được gia hạn cho các đối tượng khác

Tương tự phần IV.4.

##  Thay đổi khóa chứng thư số

Thuê bao phải có đơn xin thay đổi khóa chứng thư số.

NC-CA sẽ phải thẩm định và cấp một chứng thư số mới chứng thực cho khóa công khai thay đổi.

 Các trường hợp thay đổi khóa chứng thư số

Trước khi hết hạn chứng thư số hoặc sau khi hết hạn chứng thư số thuê bao có thể yêu cầu thay đổi khóa chứng thư số.

 Người yêu cầu thay đổi khóa chứng thư số

Thuê bao phải trực tiếp yêu cầu việc thay đổi khóa chứng thư số.

 Quy trình xử lý yêu cầu thay đổi khóa chứng thư số

Khi cần thay đổi khóa chứng thư số, thuê bao phải có đơn xin thay đổi khóa chứng thư số.

NC-CA và RA, đại lý thực hiện các trình tự thủ tục thẩm định đảm bảo xác minh chính xác người yêu cầu thay đổi khóa chứng thư số là thuê bao của chứng thư số được yêu cầu thay đổi khóa.

 Thông báo cho thuê bao

Thực hiện thông báo cho thuê bao và xác nhận với thuê bao về việc cấp chứng thư số cho khóa thay đổi của thuê bao.

 Bàn giao và xác nhận với thuê bao

NC-CA thực hiện bàn giao chứng thư số và yêu cầu thuê bao kiểm tra, xác nhận tính chính xác của thông tin thuê bao trên chứng thư số với khóa thay đổi do NC-CA cấp theo đề nghị của thuê bao.

Thuê bao phải xác nhận trước khi NC-CA công bố chứng thư số của thuê bao trên cơ sở dữ liệu danh bạ trực tuyến về chứng thư số của NC-CA.

 Công bố chứng thư số

Trong vòng 24 giờ làm việc sau khi có xác nhận của thuê bao, NC-CA tiến hành công bố chứng thư số của thuê bao trên hệ thống cơ sở dữ liệu danh bạ chứng thư số trực tuyến của NC-CA.

 Thông báo việc thay đổi khóa chứng thư số của thuê bao đến các tổ chức, cá nhân khác

Thông báo việc thay đổi khóa chứng thư số của thuê bao đến các tổ chức, cá nhân khác được thực hiện bằng cách công bố chứng thư số thuê bao trên hệ thống danh bạ trực tuyến về chứng thư số của NC-CA, và trên giấy chứng nhận do NC-CA cấp thay đổi cho thuê bao.

##  Thay đổi thông tin chứng thư số

 Các trường hợp thay đổi chứng thư số

Khi thuê bao có nhu cầu thay đổi thông tin trên chứng thư số đang sử dụng của thuê bao mà không thay đổi khóa chứng thư số.

 Người yêu cầu thay đổi chứng thư số

Thuê bao phải trực tiếp yêu cầu việc thay đổi chứng thư số.

 Quy trình xử lý yêu cầu thay đổi chứng thư số

Thuê bao phải có đơn xin thay đổi chứng thư số.

NC-CA sẽ phải thẩm định và cấp đổi một chứng thư số mới chứng thực cho khóa công của thuê bao.

NC-CA và RA, đại lý thực hiện các trình tự thủ tục thẩm định đảm bảo xác minh chính xác người yêu cầu thay đổi chứng thư số là thuê bao của chứng thư số được yêu cầu thay đổi.

 Thông báo cho thuê bao

Thực hiện thông báo cho thuê bao và xác nhận với thuê bao về việc cấp chứng thư số cho yêu cầu thay đổi chứng thư số của thuê bao.

 Bàn giao và xác nhận với thuê bao

NC-CA thực hiện bàn giao chứng thư số và yêu cầu thuê bao kiểm tra, xác nhận tính chính xác của thông tin thuê bao trên chứng thư số thay đổi với do NC-CA cấp theo đề nghị của thuê bao.

Thuê bao phải xác nhận trước khi NC-CA công bố chứng thư số thay đổi của thuê bao trên cơ sở dữ liệu danh bạ trực tuyến về chứng thư số của NC-CA.

 Công bố chứng thư số

Trong vòng 8 giờ làm việc sau khi có xác nhận của thuê bao, NC-CA tiến hành công bố chứng thư số của thuê bao trên hệ thống cơ sở dữ liệu chứng thư số trực tuyến của NC-CA.

 Thông báo việc thay đổi chứng thư số của thuê bao đến các tổ chức, cá nhân khác

Thông báo việc thay đổi chứng thư số của thuê bao đến các tổ chức, cá nhân khác được thực hiện bằng cách công bố chứng thư số thuê bao trên hệ thống danh bạ trực tuyến về chứng thư số của NC-CA, và trên giấy chứng nhận do NC-CA cấp thay đổi cho thuê bao.

##  Thu hồi và đình chỉ chứng thư số

Các tình huống thu hồi chứng thư số

Yêu cầu thu hồi chứng thư số sẽ được xử lý khi thuê bao đề nghị, do NC-CA quyết định hoặc theo yêu cầu của pháp luật.

Nếu chứng thư số đã bị thu hồi, thông tin chứng thư số bị thu hồi sẽ được công bố lên danh sách chứng thư số bị thu hồi (CRL) và cập nhật vào Cơ sở dữ liệu chứng thư số.

Cụ thể chứng thư số bị thu hồi trong những trường hợp sau:

* Thông tin trong chứng thư số được phát hiện sai khác so với thực tế.
* Khóa bí mật của thuê bao có chứng thư số bị lộ.
* Thuê bao đề nghị thu hồi.
* Chứng thư số có tên mạo danh hoặc vi phạm quyền sỡ hữu trí tuệ.
* Chứng thư số được sử dụng sai mục đích.
* Chứng thư số đã được tạo ra không tuân theo những thủ tục được yêu cầu bởi quy chế chứng thực này.
* Có lệnh dừng sử dụng chứng thư số hoặc dừng toàn bộ hệ thống.
* Theo quy định của pháp luật hay theo yêu cầu của các cơ quan có thẩm quyền.

Khi khóa bí mật của thuê bao bị mất/lộ hoặc nghi ngờ bị mất/lộ, thuê bao phải báo ngay lập tức cho NC-CA.

Ai có thể yêu cầu thu hồi chứng thư số

* Thuê bao đề nghị thu hồi chứng thư số của mình.
* Về an toàn thông tin, NC-CA có quyền yêu cầu thu hồi chứng thư số.
* Theo yêu cầu của pháp luật.

 Thủ tục thu hồi chứng thư số

Trước khi thu hồi chứng thư số, NC-CA xác thực yêu cầu thu hồi chứng thư số bằng cách:

* Thu hồi theo yêu cầu: Khi nhận yêu cầu thu hồi từ một thuê bao cho chứng thư số của mình, NC-CA sẽ kiểm tra để đảm bảo yêu cầu đó là chính xác. Trong trường hợp thuê bao thông báo khẩn cấp bằng phương tiện liên lạc như điện thoại, thư điện tử,…chỉ khi thuê bao có Đơn yêu cầu thu hồi chứng thư số có xác nhận của tổ chức, doanh nghiệp đối với tổ chức doanh nghiệp hoặc chính cá nhân và nêu rõ lý do, NC-CA mới chính thức thu hồi và công bố thông tin thu hồi chứng thư số.
* Xác minh Quyết định yêu cầu thu hồi chứng thư số của đơn vị có thẩm quyền.
* NC-CA xác minh thuê bao có sự cố gây mất an toàn như: lộ khóa, khóa không còn an toàn, …

 Thủ tục thu hồi chứng thư số

**Bước 1**: Lập hồ sơ xin thu hồi chứng thư số

Thuê bao tới đại lý hoặc RA làm hồ sơ theo mẫu, nêu rõ lý do thu hồi chứng thư số có chữ ký xác nhận của tổ chức, doanh nghiệp, văn bản ủy quyền nếu là tổ chức doanh nghiệp. Sau đó gửi hồ sơ để đề nghị thu hồi chứng thư số.

**Bước 2**: Nhập thông tin thu hồi chứng thư số

RA tiếp nhận thông tin từ đại lý, xác minh hồ sơ và nhập vào hệ thống để thực hiện việc thu hồi chứng thư số.

**Bước 3**: Thực hiện thu hồi chứng thư số

CA kiểm tra lại hồ sơ yêu cầu, nếu hồ sơ hợp lệ thì phê duyệt thu hồi chứng thư số (Approve):

* Thực hiện thu hồi chứng thư số.
* RA thực hiện kiểm tra lại trạng thái của chứng thư số sau khi thực hiện. Nếu chứng thư số có trạng thái bị thu hồi thì việc thu hồi chứng thư số của thuê bao là thành công; Thông tin về việc thu hồi của thuê bao sẽ được hệ thống lưu trữ theo quy định.

**Bước 4**: Công bố chứng thư số bị thu hồi

NC-CA thông báo tới thuê bao qua email, hoặc điện thoại , fax về việc đã thu hồi thành công chứng thư số.

Hệ thống NC-CA sẽ công bố công khai chứng thư số bị thu hồi ngay sau khi bị thu hồi thông qua dịch vụ web, CRL và OCSP theo quy định.

Trường hợp có yêu cầu thu hồi chứng thư số từ các cơ quan chức năng có thẩm quyền thì thực hiện xác minh yêu cầu và thực hiện bước 4, bước 5.

 Thời hạn gửi yêu cầu thu hồi chứng thư số

* Thuê bao sẽ gửi yêu cầu thu hồi chứng thư số ngay lập tức khi phát hiện hay nghi ngờ khóa bí mật bị mất/lộ.
* Các yêu cầu thu hồi từ các cơ quan có thẩm quyền gửi yêu cầu thu hồi chứng thư số tối thiểu 03 ngày trước thời hạn cần thu hồi chứng thư số. Trong trường hợp khẩn cấp, cần liên lạc theo các phương tiện có thể với NC-CA để tạm ngưng chứng thư số.

 Thời gian bắt đầu xử lý yêu cầu thu hồi chứng thư số

NC-CA sẽ xử lý ngay khi nhận được yêu cầu thu hồi chứng thư số hợp lệ.

 Kiểm tra trạng thái thu hồi

Người tin tưởng sẽ có được thông tin trạng thái chứng thư số, thông qua CRL và OCSP.

 Tần suất công bố CRL mới

CRL được cập nhật ít nhất một ngày một lần.

CRL được công bố ngay lập tức sau khi được tạo ra.

Chứng thư số hết hạn bị loại bỏ khỏi CRL.

 Kiểm tra trạng thái chứng thư số trực tuyến

Thông tin thu hồi và trạng thái chứng thư số được công bố qua OCSP hoặc trang Web.

Yêu cầu kiểm tra trạng thái thu hồi trực tuyến

Người nhận phải kiểm tra trạng thái của một chứng thư số nếu muốn tin tưởng.

Việc kiểm tra trạng thái chứng thư số được thực hiện thông qua CRL hay dịch vụ OCSP.

Các dạng thông tin trạng thái thu hồi khác

NC-CA không sử dụng dạng công bố thông tin trạng thái thu hồi nào khác ngoài CRL và OCSP.

Quy trình tạm dừng chứng thư số

NC-CA không thực hiện tạm dừng chứng thư số

Quy trình phục hồi chứng thư số

NC-CA không thực hiện phục hồi chứng thư số

Yêu cầu đặc biệt khi khóa CA, sub CA bị mất, bị lộ hoặc thu hồi

Khi khóa bí mật bị mất/lộ hoặc nghi ngờ mất/lộ NC-CA ngay lập tức thông báo cho các thuê bao về sự mất/lộ này thông qua các tất cả các phương tiện liên lạc có thể.

##  Dịch vụ về trạng thái chứng thư số

Phương tiện công bố

Trạng thái của chứng thư số được công bố qua CRL và OCSP.

Tính sẵn sàng của dịch vụ

Dịch vụ trạng thái chứng thư số được duy trì 24/7. Nếu có gián đoạn NC-CA sẽ thông báo trước 24 giờ.

Tùy chọn đặc biệt

Không có quy định.

## Kết thúc thuê bao chứng thư số

Yêu cầu kết thúc thuê bao chứng thư số có hiệu lực trong các trường hợp sau:

* Có lệnh dừng sử dụng chứng thư số hoặc dừng toàn bộ hệ thống NC-CA hoặc NC-CA hết thời hạn hoạt động.
* Thuê bao đã hết hạn mà không gia hạn.
* Thu hồi chứng thư số xảy ra mà không xin cấp một chứng thư số mới.

Thời hạn sử dụng của chứng thư số được chỉ rõ trong chứng thư số.

## Lưu khóa ở bên thứ ba và khôi phục khóa

Hiện tại, NC-CA không thực hiện việc lưu trữ khóa bí mật của thuê bao cũng như cung cấp dịch vụ phục hồi khóa (trừ trường hợp đặc biệt được cơ quan có thẩm quyền yêu cầu).

Duy nhất trường hợp thuê bao đăng ký chứng thư số máy chủ (SSL) được tự sinh cặp khóa bí mật theo quy trình của NC-CA.

Thuê bao phải lưuu trữ khóa bí mật vào các thiết bị an toàn (Token, Smartcard hay HSM) và tự chịu trách nhiệm về an toàn, bảo mật của khóa bí mật đó.

Chính sách và thủ tục gửi giữ khóa riêng

NC-CA không áp dụng.

Chính sách và thủ tục khôi phục gửi giữ khóa riêng

NC-CA không áp dụng.

THIẾT BỊ, QUẢN LÝ VÀ KIỂM SOÁT VẬN HÀNH

Các yêu cầu đối với cơ sở hạ tầng, tổ chức và các biện pháp an ninh của NC-CA được xác định dựa trên các loại hình dịch vụ được NC-CA cung cấp.

Tính năng của hệ thống được xem xét thông qua các các giá trị cơ bản như tính sẵn sàng, tính toàn vẹn, bảo mật và xác thực, được dựa trên các quy tắc về an toàn và bảo mật thông tin.

## Kiểm soát vật lý

Nhằm đảm bảo chất lượng dịch vụ, NC-CA thực hiện các biện pháp kiểm soát và các thủ tục kiểm soát nhằm đảm bảo an ninh vật lý của hệ thống.

Địa điểm đặt hệ thống

Hệ thống thiết bị của NC-CA được đặt như sau: trung tâm dữ liệu chính (PDC) được đặt tại Datacenter của Tập đoàn công nghệ FPT và trung tâm khôi phục thảm họa (DRDC) được đặt tại Tập đoàn công nghệ Viettel. DRDC tách biệt với PDC.

Trong hoạt động bình thường thì chỉ có PDC tương tác trực tiếp với người dùng cuối và thực hiện các dịch vụ quản lý, chứng thực chữ ký số. DRDC làm nhiệm vụ như một trung tâm backup của PDC. Trường hợp có các rủi ro mà PDC không thể tự phục hồi được thì DRDC sẽ được kích hoạt và tiếp tục cung cấp dịch vụ cho người dùng.

Truy cập vật lý

Địa điểm đặt thiết bị nằm trong khuôn viên của của Datacenter của Tập đoàn công nghệ FPT và Tập đoàn công nghệ Viettel.

Phòng đặt hệ thống CA và RA của NC-CA được ngăn cách với các hệ thống khác, với hệ thống Camera giám sát an ninh và bảo vệ 24/7.

Quyền ra vào nơi đặt thiết bị được kiểm soát bởi hệ thống khóa kết hợp sử dụng công nghệ sinh trắc học hoặc smartcard. Nhân viên bảo vệ chuyên trách có trách nhiệm ngăn chặn các truy cập từ bên ngoài ở mức vật lý.

Cụ thể, kiểm soát vật lý của hệ thống NC-CA có 5 lớp bảo mật truy cập vật lý, mỗi lớp cung cấp thêm các biện pháp kiểm soát và thiết bị an ninh vật lý chống lại xâm nhập không được phép.

1. Cửa kiểm soát của cán bộ bảo vệ.
2. Cửa kiểm soát của bảo vệ Trung tâm dữ liệu.
3. Hệ thống cửa có bảo mật của Trung tâm dữ liệu.
4. Hệ thống kiểm soát truy nhập bằng sinh trắc học hoặc smartcard, camera giám sát 24/24 tại phòng đặt máy chủ CA.
5. Phòng an toàn được kiểm soát bởi sinh trắc học hoặc smartcard, để thực hiện các thao tác tạo khóa và cấp chứng thư số cần 03 cán bộ có thẩm quyền.

Điều kiện về nguồn điện, môi trường và phòng tránh thảm họa

Hệ thống cung cấp dịch vụ của NC-CA đặt tại Datacenter của Tập đoàn công nghệ FPT và Tập đoàn công nghệ Viettel nên sử dụng nguồn điện ổn định, có hệ thống UPS (online và dự phòng), có hệ thống máy phát điện. Hệ thống máy phát điện được kiểm tra bảo dưỡng định kỳ để đảm bảo tính sẵn sàng cao nhất.

Phòng đặt máy chủ của NC-CA trang bị hệ thống điều hòa có điều khiển chính xác nhiệt độ. Hệ thống cảnh báo khi nhiệt độ, độ ẩm và khói, bụi vượt ngưỡng cho phép.

Hệ thống thiết bị của NC-CA được bố trí trên tầng cao, hạn chế tối đa sự tiếp xúc với nước kể cả khi có lũ lụt.

NC-CA được trang bị phương án phòng ngừa để cảnh báo và dập tắt lửa hay các thảm hoạ khác có thể gây cháy hay khói. Hệ thống thiết kế để phù hợp với tiêu chuẩn phòng cháy chữa cháy của Việt Nam.

### **Phương án phòng chống thiên tai**

Trong trường hợp bất khả kháng như: thiên tai, lũ lụt, động đất,… mà trung tâm NC-CA chính không thể hoạt động được, kịch bản đưa trung tâm NC-CA dự phòng vào khai thác thay thế chức năng của trung tâm chính diễn ra như sau:

* Kiểm tra tính toàn vẹn của các cơ sở dữ liệu trên trung tâm CA dự phòng đến thời điểm bị sự cố.
* Khôi phục cơ sở dữ liệu (nếu cần thiết).
* Đưa hệ thống sao lưu vào hoạt động.
* Kiểm tra sự hoạt động của hệ thống.
* Thay đổi các tham số bản ghi trong máy chủ DNS để chuyển hướng truy cập sang hệ thống CA tại trung tâm CA dự phòng.
* Trung tâm dự phòng CA sẽ chuyển sang đảm nhiệm chức năng là trung tâm chính là sau khi trung tâm chính không thể hoạt động được vì bất cứ nguyên nhân nào.

### **Phương án phòng cháy chữa cháy**

Các datacenter của FPT và Viettel được trang bị hệ thống báo cháy tự động, có hệ thống xả khí chữa cháy. Ngoài ra tại nơi đặt máy chủ được trang bị thêm thêm bình bột, bình bọt chữa cháy được đặt treo trên tường ở độ cao 0,25m so với mặt sàn. phương tiện chữa cháy ban đầu khi mới phát hiện được đám cháy, người ta dùng bình bột, bình bọt chữa cháy xách tay để phun vào đám cháy ngăn cách đám cháy với ôxy (02) ngoài môi trường xung quanh để dập tắt đám cháy. Các bình bột MFZ4, bình khí CO2 MT3 chỉ dập tắt được các đám cháy nhỏ, do đó nó chỉ được dùng làm phương tiện chữa cháy ban đầu, nếu đám cháy không tắt thì phải kích hoạt hệ thống chữa cháy chủ đạo.

Phương tiện lưu trữ dữ liệu

NC-CA có phương tiện lưu trữ dữ liệu (máy chủ, hệ thống SAN) được bảo vệ khỏi nước, lửa hay môi trường huỷ hoại và được bảo vệ tránh sử dụng truy cập trái phép hay phá huỷ.

Xử lý rác

Các tài liệu chứa thông tin nhạy cảm được hủy bằng các biện pháp phù hợp trước khi được bỏ đi. Đảm bảo các thông tin nhạy cảm, ví dụ như các bản sao hồ sơ của các thuê bao, tài liệu quản lý thuê bao, phương tiện điện tử lưu dữ liệu,… khi bị hủy không thể đọc được.

Hệ thống dự phòng ở địa điểm khác

NC-CA thực hiện việc lưu trữ dữ liệu dự phòng tại DRDC. Có chế độ bảo dưỡng sao lưu dữ liệu quan trọng hay bất kỳ thông tin nhạy cảm nào phục vụ cho hoạt động của hệ thống NC-CA.

## Các thủ tục kiểm soát

Những cá nhân được tin tưởng

Người được tin tưởng là các cán bộ của NC-CA được quyền thực hiện các nhiệm vụ quan trọng như sau trong quá trình vận hành hệ thống NC-CA:

* Xác minh và kiểm tra tính đầy đủ của thông tin trong đơn xin cấp chứng thư số của các thuê bao.
* Chấp nhận, loại bỏ đơn xin cấp chứng thư số, yêu cầu thu hồi, làm mới, tạm ngưng, gia hạn chứng thư số.
* Tạo khóa, ban hành, thu hồi, tạm ngưng, gia hạn chứng thư số.
* Quản lý thông tin thuê bao.

Người được tin tưởng trong NC-CA bao gồm nhưng không giới hạn trong các đối tượng sau:

1. Người đứng đầu hệ thống.
2. Những người quản lý khóa của hệ thống.
3. Người quản trị hệ thống và bộ phận quản trị hệ thống.
4. Người phụ trách cấp phát, quản lý chứng thư số và bộ phận phụ trách quản lý chứng thư số.
5. Kiểm toán kỹ thuật
6. Quản lý lưu dữ liệu

Những người được tin tưởng đều được xác minh về nhân thân, khả năng đảm bảo đáp ứng yêu cầu công việc trước khi được giao nhiệm vụ.

Trong hệ thống còn có thể có các thành viên khác với các chức năng khác. Ví dụ như người phụ trách kiểm toán kỹ thuật.

Số người được yêu cầu trên một nhiệm vụ nhạy cảm

NC-CA đảm bảo có nhiều người được tin tưởng thực hiện một công việc nhạy cảm như truy cập, điều khiển thiết bị phần cứng mã hóa. Với các chức năng này, NC-CA có ít nhất 3 người để thực hiện cùng một công việc nhạy cảm theo mô hình “M out of N” (Mô hình này đòi hỏi ít nhất M quản trị viên trong tổng số N người sử dụng smart card/token của mình để thực hiện các thao tác quản trị và vận hành quan trọng).

Nhận dạng và xác thực trong mỗi vai trò

Mọi cá nhân trước khi trở thành người được tin tưởng trong hệ thống NC-CA phải được xác minh nhân thân, nhận dạng và trình độ lại ngoài việc đáp ứng các tiêu chuẩn. NC-CA phê duyệt danh sách các cán bộ này.

Quá trình kiểm tra lại được trình bày trong phần V.3.1.

Những vai trò yêu cầu phải phân tách nhiệm vụ

Nhằm đảm bảo an toàn thông tin, tránh các sự cố bảo mật liên quan đến nhân sự, một số vai trò cần phải có sự phân tách, bao gồm nhưng không giới hạn:

* Xác minh thông tin trong đơn xin cấp chứng thư số;
* Chấp nhận, từ chối hay các xử lý khác đối với đơn xin cấp chứng thư số, yêu cầu thu hồi, làm mới chứng thư số;
* Tạo khóa, ban hành, thu hồi chứng thư số;
* Quản lý thông tin, yêu cầu của thuê bao;
* Kiểm toán kỹ thuật của hệ thống (tùy chọn).

## Kiểm soát nhân sự

Khả năng chuyên môn, kinh nghiệm và sự trong sạch

Những cán bộ được tin tưởng của NC-CA phải được xác minh dựa trên khả năng và kinh nghiệm chuyên môn đáp ứng các nhu cầu công việc và trong sạch về lý lịch.

Các thủ tục kiểm tra lý lịch, trình độ

Trước khi được bổ nhiệm, cán bộ được tin tưởng cần được kiểm tra các thông tin sau:

* Xác minh lại trình độ học vấn cao nhất đạt được, chuyên ngành;
* Xem xét các thông tin tiền án/tiền sự/kỷ luật/tố cáo.

Yêu cầu đào tạo vận hành hệ thống

Tất cả các cán bộ liên quan đến vận hành hệ thống NC-CA được đào tạo các nội dung liên quan đến chữ ký số và chứng thực chữ ký số.

Quá trình đào tạo chuyên môn cần được ghi lại để đảm bảo nhân sự có được đầy đủ kiến thức về lĩnh vực được phân công phụ trách.

Chương trình huấn luyện của NC-CA cần hướng đến đảm bảo thực hiện được các nhiệm vụ mỗi cá nhân được giao, bao gồm nhưng không hạn chế trong các lĩnh vực sau đây:

* Các nội dung pháp lý cần thiết liên quan đến chữ ký số và giao dịch điện tử;
* Khái niệm và kiến thúc PKI cơ bản;
* Các chính sách và quy chế của NC-CA;
* Sử dụng và vận hành các thiết bị;
* Xử lý các sự cố và thủ tục duy trì tính liên tục của hệ thống.

Việc đào tạo được duy trì và đảm bảo cập nhật các kiến thức cần thiết để các nhân viên thành thạo và thực hiện tốt công việc được giao khi vận hành hệ thống NC-CA.

NC-CA đầu tư cung cấp các tài liệu cần thiết cho nhân viên để đảm bảo hoàn thành các nhiệm vụ được giao.

 Nhu cầu và tần suất đào tạo

Tổ chức hướng dẫn và đào tạo cho cán bộ mới, các cập nhật, nâng cấp hệ thống.

NC-CA tổ chức đào tạo, bồi dưỡng và cập nhật cho cán bộ của mình trong phạm vi và tần suất hợp lý để đảm bảo rằng cán bộ duy trì mức độ yêu cầu về trình độ để thực hiện trách nhiệm công việc một cách thành thạo và thỏa đáng.

Đào tạo khắc phục hậu quả được thực thi khi có khuyến cáo và kiến nghị của kiểm tra kiểm toán.

Tần suất luân chuyển công việc

Theo quy định luân chuyển cán bộ của công ty cổ phần hỗ trợ doanh nghiệp và đầu tư HN.

Xử phạt các hành động không được phép

Xử lý theo quy định của công ty cổ phần hỗ trợ doanh nghiệp và đầu tư HN và các quy định của luật pháp liên quan.

 Yêu cầu đối với nhà thầu

NC-CA không áp dụng.

 Tài liệu cấp cho cán bộ

Mỗi cán bộ thực hiện một vai trò nhất định sẽ được đào tạo và cung cấp đầy đủ tài liệu hướng dẫn vận hành, quy định, trách nhiệm và các thủ tục cho từng vai trò, nhiệm vụ để thực thi một cách thành thạo và thỏa đáng.

Phối hợp với Trung tâm Chứng thực điện tử quốc gia

NC-CA duy trì hoạt động trao đổi thông tin, chuyên môn với Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia (do Trung tâm Chứng thực điện tử quốc gia vận hành) để đảm bảo được cập nhật các thông tin liên quan đến pháp lý, chuẩn, quy định của nhà nước nhằm vận hành hệ thống cấp và quản lý chứng thư số được an toàn, đáp ứng yêu cầu.

## Quy trình lưu nhật ký kiểm toán hệ thống NC-CA

Các loại sự kiện được ghi lại

NC-CA ghi lại nhật ký (log) các sự kiện sau:

* Các sự kiện về quá trình sử dụng chứng thư số:
	+ Tạo khóa, đăng ký, tạo mới, đổi khóa, thay đổi, và thu hồi chứng thư số cho các thuê bao.
	+ Kết quả khi xử lý những yêu cầu từ các tổ chức, cá nhân muốn đăng ký chứng thư số.
	+ Ban hành CRL.
* Các sự kiện liên quan đến an toàn, an ninh:
	+ Truy cập hệ thống bởi nhân viên vận hành và của thuê bao (thành công/không thành công).
	+ Hành động đọc, ghi hoặc xóa các file, bản ghi an ninh nhạy cảm.
	+ Sự cố hệ thống và những hiện tượng bất thường.
	+ Hoạt động của an ninh mạng.
	+ Thiết bị giám sát an ninh vật lý.
* Hệ thống của NC-CA ghi lại các thông tin đăng ký bao gồm tài liệu nhận dạng được người/tổ chức xin cấp chứng thư số đưa ra, cụ thể:
	+ Thông tin định danh (xem III.2.2);
	+ Nơi lưu trữ các bản sao đơn đăng ký và tài liệu nhận dạng;
	+ Người trực tiếp xử lý, tiếp nhận đơn.

Tần suất xử lý nhật ký kiểm toán

* Nhật ký kiểm toán của hệ thống NC-CA được kiểm tra khi có sự việc không bình thường xảy ra;
* Hàng tuần nhật ký kiểm toán cần được tổng kết bằng văn bản;
* Tổng kết nhật ký kiểm toán cần được gửi đến Lãnh đạo của NC-CA.

Thời hạn giữ lại các nhật ký kiểm toán

* Nhật ký kiểm toán sẽ được giữ tại hệ thống ít nhất 6 tháng, sau đó được lưu bởi hệ thống lưu trữ (phần V.5.2).

Bảo vệ các nhật ký kiểm toán

* Nhật ký kiểm toán theo từng tháng được ký bởi lãnh đạo của NC-CA, được bảo vệ với trước các hành động xem, thay đổi, xóa bởi các đối tượng không có thẩm quyền.

Các thủ tục dự phòng nhật ký kiểm toán

* Nhật ký kiểm toán được sao lưu theo chế độ sao lưu chung của NC-CA.

Phương thức ghi nhật ký kiểm toán

* Hoạt động của hệ thống, hệ điều hành và mạng được ghi lại và có cơ chế để không thay đổi được nhật ký.
* Một số nhật ký được ghi bằng tay bởi nhân viên nếu cần bổ sung.

Thông báo cho đối tượng gây ra sự kiện

* Khi một sự kiện được ghi nhật ký kiểm toán, tùy vào bản chất sự kiện, người lãnh đạo cấp trên (xem V.4.4) có thể thông báo hoặc không thông báo cho đối tượng gây ra sự kiện đó.

Đánh giá lỗ hổng hệ thống

* Dữ liệu nhật ký kiểm toán của NC-CA được phân tích để có phương án khắc phục nếu có sự cố.

## Lưu trữ các bản ghi

Các loại bản ghi được lưu trữ

* Mọi dữ liệu nhật ký kiểm toán trong phần V.4.
* Thông tin liên quan đến đơn xin cấp chứng thư số, và vòng đời chứng thư số như: thu hồi, đổi khóa, làm mới…
* Thông tin về sử dụng chứng thư số như việc truy cập để xác định tính hiệu lực của chứng thư số (tùy chọn).
* Thông tin về các hoạt động kiểm toán kỹ thuật của hệ thống.

Thời hạn giữ lại các lưu trữ

* Thời gian lưu trữ các bản ghi theo quy định của pháp luật. Nếu không có quy định, thời gian lưu trữ ít nhất là 10 năm.

Bảo vệ lưu trữ

* Hệ thống lưu dữ liệu lưu trữ của NC-CA được bảo vệ để chỉ những người được phép mới có thể truy nhập.
* Dữ liệu lưu trữ được bảo vệ theo các phương pháp cần thiết, chống lại việc xem, thay đổi, xóa hay các thao tác khác không được cho phép.
* Hệ thống chứa dữ liệu lưu trữ và ứng dụng xử lý dữ liệu lưu trữ được duy trì để đảm bảo dữ liệu lưu trữ có thể được truy nhập trong khoảng thời gian hệ thống NC-CA được phép hoạt động.

Các thủ tục sao lưu lưu trữ

Dữ liệu lưu trữ được tiến hành sao lưu theo chế độ sao lưu của NC-CA.

Nhãn thời gian của các bản ghi

Các bản ghi có chứa thông tin về thời gian, ngày tháng.

Thông tin thời gian không cần được mã hóa.

Hệ thống lưu trữ

Hệ thống lưu trữ của NC-CA là hệ thống tập trung, có dự phòng.

Thủ tục truy cập và kiểm tra thông tin lưu trữ

Chỉ những người được cấp quyền mới được phép truy nhập tới thông tin lưu trữ của hệ thống NC-CA.

## Thay đổi khóa của NC-CA

Trước khi chứng thư số của NC-CA hết hạn, nếu trong thời gia được cấp phép, NC-CA sẽ đăng ký với RootCA để được gia hạn và sử dụng chứng thư số mới và cặp khóa mới để ban hành chứng thư số cho các thuê bao.

Chỉ có khóa mới nhất của NC-CA là được sử dụng cho mục đích ký các chứng thư số.

Các khóa trước khi vẫn cần được lưu trữ để kiểm tra các chữ ký và để ký CRL.

Thời gian hoạt động của chứng thư số của NC-CA và thời gian sử dụng cặp khoá được quy định trong phần VI.3.2.

## Lộ khóa và khôi phục sự cố/thảm họa

Các thủ tục kiểm soát sự cố và thảm họa

NC-CA có một Hướng dẫn Xử lý các tình huống khẩn cấp khi có các sự cố về an toàn thông tin và việc lộ cặp khóa của NC-CA.

Tài liệu Hướng dẫn Xử lý các tình huống khẩn cấp cần được chuyển đến tay tất cả các cán bộ của NC-CA.

Các yếu tố cơ bản của các thủ tục trong Hướng dẫn Xử lý các tình huống khẩn cấp được bao gồm các mục V.7.2, V.7.3.

Sự cố về máy tính, phần mềm và dữ liệu

Khi có các sự cố về máy tính, phần mềm và dữ liệu, các thủ tục xử lý sự cố được thực hiện.

Hệ thống sẽ được khởi động lại dựa trên phần cứng dự phòng bằng cách sử dụng phần mềm sao lưu và dữ liệu được sao lưu tại DRDC của NC-CA, sau đó sẽ được kiểm tra và đưa vào hoạt động trong một điều kiện đảm bảo an toàn.

Hệ thống máy tính bị lỗi sau đó sẽ được phân tích tìm sự cố.

Nếu cần thiết, thêm các biện pháp bảo vệ cũng sẽ được đưa ra để ngăn chặn sự xuất hiện của sự cố tương tự trong tương lai.

NC-CA có các hợp đồng với các chuyên gia về PKI để phân tích các sự cố này.

NC-CA thông báo với Trung tâm Chứng thực điện tử quốc gia về sự cố này không muộn quá 01 ngày làm việc kể từ khi sự cố xảy ra, theo các quy định của thông tư số 37/2009/TT-BTTTT và Thông tư số 08/2011/TT-BTTTT do Bộ Thông tin truyền thông ban hành.

Thủ tục xử lý khi khóa bí mật bị làm mất/lộ

Khi có nghi ngờ khóa bí mật của NC-CA bị lộ hay bị mất, ngay lập tức cần báo động cho toàn bộ nhân viên của NC-CA, từ người đứng đầu, người phụ trách kỹ thuật và người phụ trách cấp phát chứng thư số đến các nhân viên kỹ thuật khác. Các bước sau cần được tiến hành:

1. Thông báo ngay lập tức với lãnh đạo công ty cổ phần hỗ trợ doanh nghiệp và đầu tư HN (thông báo cho Trung tâm Chứng thực điện tử quốc gia và các cơ quan pháp luật có liên quan) để phối hợp loại bỏ các chứng thư số bị ảnh hưởng từ sự cố.
2. Thông báo ngay lập tức cho tất cả các thuê bao bị ảnh hưởng bằng mọi phương tiện có thể.
3. Thu hồi ngay lập tức tất cả chứng thư số đã phát hành. Rà soát các thông tin online, được lưu trữ, hay các dữ liệu kiểm toán kỹ thuật. Khi cần, kho dữ liệu của NC-CA cần được ngắt off-line để hạn chế các thông tin không chính xác được công bố.
4. Tổ chức tạo một cặp khoá mới và chứng thư số mới cho NC-CA.
5. Duy trì hoạt động cấp các chứng thư số mới cho thuê bao.

Khả năng phục hồi hoạt động sau thảm họa

NC-CA cần có kế hoạch dự phòng, đảm bảo hoạt động liên tục kể cả có thảm họa hay sự cố lớn. Các kế hoạch này cần được kiểm tra, thử nghiệm và xem xét định kỳ.

NC-CA có khả năng phục hồi những hoạt động quan trọng sau đây trong vòng 01 ngày làm việc sau khi một thảm họa xảy ra.

1. Công bố thông tin thu hồi chứng thư số;
2. Ban hành chứng thư số;
3. Thu hồi chứng thư số.

NC-CA dự phòng các thiết bị phần cứng và phần mềm cung cấp dịch vụ. Khóa bí mật của NC-CA cũng được dự phòng và duy trì phục vụ cho mục đích phục hồi hệ thống như phần VI.2.4.

## Kết thúc CA và RA

Khi chấm dứt hoạt động, NC-CA hoặc RA sẽ báo cho thuê bao, người tin cậy và các đối tượng có liên quan trước khi dừng hoạt động 06 tháng.

Nếu vì lý do cần dừng để chuyển sang sử dụng dịch vụ của các tổ chức cung cấp dịch vụ chứng thực chữ ký số khác, NC-CA cần:

* Thông báo cho các thuê bao bị ảnh hưởng;
* Thu hồi chứng thư số của thuê bao, nếu cần thiết;
* Thực hiện các thủ tục chuẩn bị, hướng dẫn các thuê bao chuyển sang tổ chức cung cấp dịch vụ chứng thực chữ ký số khác;
* Bảo quản dữ liệu lưu trữ và bản ghi của NC-CA trong thời gian được quy định bởi quy chế này;
* Tiếp tục dịch vụ hỗ trợ thuê bao tới khi các chứng thư số do NC-CA ban hành hết hạn, nếu cần thiết.

KIỂM SOÁT AN TOÀN KỸ THUẬT

## Tạo cặp khóa và cài đặt

Sinh cặp khóa

* Cặp khóa cho NC-CA được sinh ra trong thiết bị phần cứng mã hóa chuyên dụng (Hardware Security Module) đạt chuẩn FIPS 140-2 level 3 trở lên.
* Cặp khóa của thuê bao được sinh trực tiếp và lưu trên các thiết bị chuyên dụng do thuê bao giữ.

Chuyển giao khóa bí mật cho khách hàng

* Cặp khóa của khách hàng (hay thuê bao) được sinh ra tại thiết bị USB token do NC-CA cung cấp. NC-CA thực hiện thủ tục sinh cặp khóa trong thiết bị tại NC-CA và phân phối thiết bị trực tiếp tới khách hàng hoặc qua RA.
* Thiết bị USB token sẽ sinh cặp khóa cho người sử dụng sử dung thuật toán sinh khóa RSA với các tham số an toàn, độ dài khóa ít nhất 2048bit

 Chuyển giao khóa công khai của thuê bao đến NC-CA

* NC-CA, RA, đại lý hoặc thuê bao chuyển giao tệp tin đề nghị cấp chứng thư số cho thuê bao mã theo chuẩn PKCS #10 sinh từ PKI Smartcard, PKI Token, PKI Virtual Token đạt chuẩn FIPS 140-2 Level 2 trở lên, hoặc tương đương qua kênh bảo mật SSL.

Công bố chứng thư số của NC-CA

* Người nhận có thể tải về khóa công khai của NC-CA từ trang Web của dịch vụ NC-CA.
* Đường dẫn http://pub.nc-ca.vn/certs/nc-ca.cer

Độ dài khóa

* NC-CA tạo các cặp khóa có độ dài tối thiểu 2048 bits RSA cho các chứng thư số của thuê bao.
* Cặp khóa của NC-CA có độ dài tối thiểu 2018 bit RSA.

Các tham số sinh cặp khóa mã công khai và kiểm tra chất lượng

* Quá trình sinh cặp khóa mã công khai được tiến hành tuân theo thuật toán RSA chuẩn PKCS #1.
* NC-CA tuân thủ tiêu chuẩn về chữ ký số và chứng thực chữ ký số do Bộ Thông tin và Truyền thông ban hành. Phiên bản gần nhất của các tiêu chuẩn này là thông tư 06/2015/TT-BTTTT ngày 23 tháng 3 năm 2015.

 Mục đích sử dụng khóa (theo X.509 V3)

* Trường mở rộng về mục đích sử dụng khóa trong chứng thư số của thuê bao do NC-CA cấp quy định về hạn chế các mục đích sử dụng mà thuê bao được áp dụng.
* Cặp khóa ký số được sử dụng để cung cấp xác thực, tính toàn vẹn và chống từ chối.
* Cặp khóa mã hóa được sử dụng cho mục đích mã hóa dữ liệu, phục vụ bảo mật.

##  Bảo vệ khóa bí mật và kiểm soát module mã hóa

Tiêu chuẩn module mã hóa

* Thiết bị phần cứng mã hóa chuyên dụng HSM được dùng để lưu trữ khóa bí mật của NC-CA. Thiết bị HSM của NC-CA đáp ứng tiêu chuẩn FIPS 140-2 level 3 trở lên.

Lưu giữ ngoài khóa bí mật của thuê bao

* Quy định về lưu giữ ngoài khóa bí mật (key escrow) của thuê bao được trình bày trong phần IV.12.

Cơ chế kiểm soát khóa bí mật

* Khóa bí mật của NC-CA được tách thành N phần khác nhau, các phần này được giữ bởi các đối tượng khác nhau. Với mỗi chức năng, cần có M phần (M nhỏ hơn hay bằng N) mã chia sẻ để kích hoạt chứng năng đó.
* Đối với NC-CA, N = 5, M= 3;

Dự phòng khóa bí mật

* NC-CA sẽ lưu dự phòng (backup) khóa bí mật của mình để đề phòng thảm họa và trục trặc thiết bị. Khóa bí mật của NC-CA được lưu trữ trong các thiết bị HSM.

Lưu trữ khóa bí mật

* Sau khi hết thời hạn hoạt động, cặp khóa của NC-CA vẫn được lưu trữ (archive) an toàn với thời hạn ít nhất 5 năm trong HSM nhằm mục đích tra cứu sau này theo yêu cầu của cơ quan có thẩm quyền.

Chuyển khóa bí mật vào/ra HSM

* Khóa bí mật ở ngoài HSM luôn ở trạng thái mã. NC-CA không lưu khóa ngoài HSM.

 Phương pháp giữ khóa riêng NC-CA

* Khối bảo mật phần cứng HSM 140-2 Level 3 chịu tách nhiệm giữ khóa riêng phục vụ cho hoạt động của hệ thống NC-CA.

Phương thức kích hoạt khóa bí mật

* NC-CA sẽ có các biện pháp kỹ thuật bảo vệ kích hoạt khóa bí mật phù hợp với yêu cầu của thuê bao. Khóa bí mật được lưu trong token/smartcard do thuê bao giữ. Việc kích hoạt khóa bí mật yêu cầu mật khẩu bảo vệ (PIN).
* Hệ thống NC-CA sử dụng HSM để lưu trữ khóa bí mật và việc kích hoạt khóa bí mật yêu cầu các mã chia sẻ theo cơ chế chia sẻ mã trong VI.2.3.

Phương pháp ngừng kích hoạt khóa bí mật

* Các thành viên của NC-CA được yêu cầu phải đăng xuất khỏi hệ thống khi rời chỗ làm việc.
* Khóa bí mật của quản trị hệ thống, của RA phải bị ngừng kích hoạt sau mỗi nhiệm vụ, sau khi đăng xuất hệ thống hoặc sau khi rút token/smartcard khỏi máy tính.

Phương pháp hủy bỏ khóa bí mật

* Việc xóa khóa bí mật được thực hiện theo phương pháp an toàn, đảm bảo không thể phục hồi lại khóa đã xóa.
	+ Khóa bí mật lưu trên token/smartcard được xóa bằng phần mềm quản trị chuyên dụng. NC-CA hướng dẫn cho các cán bộ vận hành và thuê bao cách thức hủy bỏ khóa bí mật khi cần thiết;
	+ Khóa bí mật của NC-CA lưu trên HSM được xóa bằng chứng năng xóa khóa của HSM.
* Các hoạt động hủy bỏ khóa bí mật, liên quan đến hệ thống CA hoặc của các cán bộ được giao vận hành hệ thống CA, được ghi lại trong nhật ký.

Đánh giá thiết bị mã hóa phần cứng

* Xem phần VI.2.1.

## Các vấn đề khác của việc quản lý cặp khóa

Lưu trữ khóa công khai

NC-CA sẽ lưu trữ khóa công khai của mình và toàn bộ thuê bao.

Thời hạn sử dụng chứng thư số và thời hạn sử dụng cặp khóa

Thời hạn sử dụng của chứng thư số sẽ kết thúc khi chứng thư số đó hết hạn hoặc bị thu hồi.

Thời hạn sử dụng cặp khóa của thuê bao giống như thời hạn sử dụng của chứng thư số, ngoại trừ chức năng giải mã và kiểm tra chữ ký sau khi chứng thư số hết hạn.

NC-CA không ban hành các chứng thư số có thời hạn sử dụng vượt quá thời hạn sử dụng chứng thư số của NC-CA.

Chứng thư số mà NC-CA cung cấp cho thuê bao thông thường là 01 năm. Chứng thư số cũng có thể kéo dài đến 03 năm với các điều kiện sau:

* Thuê bao được yêu cầu thực hiện lại các thủ tục xác thực ít nhất 12 tháng một lần (phần III.2.3, III.2.4).
* Thuê bao phải chứng minh quyền sở hữu khóa bí mật.

Nếu điều kiện trên không được thực hiện, NC-CA sẽ tự động thu hồi chứng thư số của thuê bao.

##  Dữ liệu kích hoạt

Tạo và cài đặt dữ liệu kích hoạt

Dữ liệu kích hoạt khóa bí mật của NC-CA được chia thành các mã được chia sẻ.

Các mã được chia sẻ này được tạo theo các yêu cầu trong phần VI.2.3 và tuân theo các thủ tục, quy định về Lễ sinh khóa của một CA.

 Quá trình tạo và phân phối mã chia sẻ được ghi nhật ký.

Mật khẩu để bảo vệ, kích hoạt khóa chia sẻ được đặt theo nguyên tắc mật khẩu mạnh.

 Bảo vệ dữ liệu kích hoạt

Người giữ mã chia sẻ của NC-CA được yêu cầu bảo vệ an toàn mã chia sẻ của họ. Những người này phải ký một thỏa thuận với NC-CA về việc đảm bảo trách nhiệm trong việc bảo vệ mã chia sẻ mà họ giữ.

RA và quản trị hệ thống được yêu cầu phải giữ khóa bí mật ở dạng mã hóa sử dụng mật khẩu bảo vệ.

Thuê bao của NC-CA được yêu cầu lưu trữ khóa bí mật dưới dạng mã hóa sử dụng Token/smartcard và mật khẩu bảo vệ.

Các vấn đề khác của dữ liệu kích hoạt

* Truyền, gửi dữ liệu kích hoạt

Dữ liệu kích hoạt khi được truyền, gửi đi được bảo vệ chống lại việc mất, lộ, truy nhập không được phép.

* Hủy bỏ dữ liệu kích hoạt

Sau khi hết hạn sử dụng được quy định trong phần V.5.2, NC-CA sẽ loại bỏ dữ liệu kích hoạt khóa bí mật bằng cách ghi đè và/hoặc hủy bỏ vật lý.

##  Kiểm soát an ninh cho hệ thống máy tính

Hệ thống NC-CA được vận hành với các biện pháp đảm bảo an ninh do công ty cổ phần hỗ trợ doanh nghiệp và đầu tư HN quy định.

Các yêu cầu an ninh hệ thống máy tính

Các máy chủ cài đặt hệ thống NC-CA và dữ liệu được bảo vệ khỏi các truy nhập không được phép.

NC-CA giới hạn quyền truy nhập tới máy chủ CA theo vai trò của quản trị.

Trên các máy tạo cặp khóa của NC-CA, không kết nối vào mạng và không cài đặt các ứng dụng khác.

Hệ thống mạng của NC-CA được cách ly với các hệ thống khác, bảo vệ khỏi sự truy cập bất hợp pháp, được thiết kế theo mô hình 4 vùng (DMS, Service, CA và WAN-Internet). Sự cách ly này được thực hiện bằng hệ thống tường lửa. Lớp tường lửa và IPS bên ngoài bảo vệ cả hệ thống khỏi các truy nhập từ ngoài. Lớp tường lửa bên trong cách ly các máy chủ CA và hệ thống mạng chung của NC-CA.

NC-CA yêu cầu sử dụng mật khẩu mạnh, được định kỳ được thay đổi.

Việc truy nhập trực tiếp dữ liệu của CA chỉ được giới hạn cho những người có quyền và nhiệp vụ phù hợp.

Đánh giá an ninh của hệ thống máy tính

Đánh giá theo quy định của công ty cổ phần hỗ trợ doanh nghiệp và đầu tư HN.

##  Kiểm soát kỹ thuật vòng đời chứng thư số

Giám sát triển khai hệ thống

NC-CA đáp ứng các điều kiện được quy định trong thông tư 06/2015/TT-BTTTT về danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số.

Quá trình triển khai và khai thác hệ thống chịu sự giám sát chặt chẽ của NC-CA.

Quản lý giám sát an ninh

NC-CA có các thủ tục và biện pháp kiểm soát an ninh trong quá trình thiết lập hệ thống phù hợp với các quy định nội bộ.

Các cấu hình của hệ thống CA cũng như bất kỳ sửa đổi và nâng cấp phải được ghi chép và kiểm soát. Có phương pháp phát hiện sửa đổi trái phép các phần mềm CA hay cấu hình.

Giám sát an ninh vòng đời chứng thư số

NC-CA tuân thủ quy trình trong cả vòng đời chứng thư số.

##  Kiểm soát an toàn mạng

NC-CA phải được bảo vệ khỏi bị tấn công thông qua bất kỳ mạng mở hoặc mạng dùng riêng mà nó được kết nối.

Bảo vệ này phải được cung cấp thông qua việc lắp đặt thiết bị và cấu hình để cho phép chỉ có các giao thức và lệnh cần thiết cho hoạt động của CA mới được chấp nhận.

##  Cấp dấu thời gian

NC-CA chưa thực hiện dịch vụ cấp dấu thời gian.

Với nhãn thời gian cho các bản ghi, NC-CA thực hiện theo mục V.5.5

Với thời gian trong từng ứng dụng, NC-CA tuân thủ quy định của ứng dụng (sử dụng thời gian trên máy client hoặc server tùy theo ứng dụng cụ thể).

ĐỊNH DẠNG CHỨNG THƯ SỐ, CRL VÀ OCSP

## Hồ sơ chứng thư số

Phiên bản

Chứng thư số do NC-CA ban hành tuân theo chuẩn ITU-T X.509 v3 và các quy định của RFC 5280.

Trường cơ bản

Chứng thư số do NC-CA ban hành có các trường cơ bản theo bảng dưới đây.

|  |  |
| --- | --- |
| **Trường Giá trị** | **Ý nghĩa** |
| Serial Number | Giá trị là duy nhất đối với mỗi chứng thư số do NC-CA ban hành |
| Signature Algorithm | Định danh (OID) của thuật toán được sử dụng để ký lên chứng thư số  |
| Issuer  | NC-CA |
| Valid From | Thời điểm bắt đầu chứng thư số có hiệu lực, theo giờ Việt nam |
| Valid To | Thời điểm hết hiệu lực của chứng thư số, theo giờ Việt nam |
| Subject DN | Xem phần VII.1.5 |
| Subject Public key | Khóa công khai, được mã hóa phù hợp với RFC 5280 |
| Signature | Chữ kýsố của NC-CA được mã hóa phù hợp với RFC 5280 |

Trường mở rộng

NC-CA phải công bố các phần mở rộng của chứng thư số và các ứng dụng đã được phê duyệt phải xử lý các mở rộng này như quy định tại RFC5280.

Phần mở rộng của chứng thư số được NC-CA hỗ trợ bao gồm:

* Basic Contraints (basicContraints): chứa thông tin xác định đây có phải là CA không và độ sâu lớn nhất của cấu trúc phân cấp chứng thư (certificate path).
* Key Usage (keyUsage): mô tả mục đích sử dụng của khóa được lưu trong chứng thư.
* Certificate Policies (certificatePolicies): chứa một hoặc nhiều cụm các thông tin chính sách, mỗi cụm gắn kèm với nó là một OID và một bộ định tính tùy chọn (optional qualifiers).

* Authority Key Identifier (authorityKeyIdentifier): xác định khóa công khai tương ứng với khóa bí mật đã sử dụng để ký CRL.
* Subject Key Identifier (subjectKeyIdentifier): xác định các chứng thư chứa một khóa công khai cụ thể.
* CRL Distribution Points (crlDistributionPoints): chứa các thông tin về danh sách thu hồi chứng thư (CRL).
* Authority Information Access (authorityInforaccess): đưa ra cách truy cập các thông tin và dịch vụ CA của nhà cung cấp theo các trường mở rộng của chứng thư.
* Extended Key Usage (extendedKeyUsage): đưa ra một hoặc nhiều các mục đích sử dụng của khóa bổ xung cho mục đích sử dụng xác định trong mục Key Usage.

Các thuật toán ký

NC-CA sử dụng thuật toán ký RSA với hàm băm SHA256

Khuôn dạng tên

Chứng thư số của NC-CA chứa tên phân biệt (DN) dạng X.509 đầy đủ của NC-CA và certificate subject trong các trường issuer name và subject name.

Tên phân biệt (DN) ở dạng của một chuỗi ký tự in được của X.501.

Giới hạn tên

NC-CA không có giới hạn tên nào.

Sử dụng ràng buộc mở rộng chính sách chứng thư số

OID của Quy chế chứng thực này được xác định

1.3.6.1.4.1.30339.1.[code-CA].3

[code-CA] do Bộ Thông tin và Truyền thông cấp.

Cú pháp và ngữ nghĩa của chính sách phân loại

Không quy định.

Xử lý ngữ nghĩa của các trường mở rộng chính sách chứng thư số

Không quy định.

## Hồ sơ CRL

CRL do NC-CA công bố tuân theo chuẩn ITU-T X.509 v3 và các quy định của RFC 5280. Tối thiểu, CRL do NC-CA công bố có các trường và giá trị theo bảng dưới đây:

|  |  |
| --- | --- |
| **Trường Giá trị** | **Ý nghĩa** |
| Serial Number | Xem phần VII.2.1 |
| Signature Algorithm | Thuật toán được dùng để ký CRL. Sử dụng một trong các hàm băm sau SHA-256, SHA-384, SHA-512.  |
| Issuer  | Thực thể ký và ban hành CRL: NC-CA |
| Effective Date | Ngày có hiệu lực của CRL. |
| Next Update | Thời gian mà CRL tiếp theo sẽ được công bố. |
| Revoked Certificates | Danh sách các chứng thư số bị thu hồi, bao gồm Serial Number của các chứng thư số bị thu hồi và ngày thu hồi. |

Số phiên bản của CRL

NC-CA ban hành X.509 V3 CRL.

CRL và các trường mở rộng của CRL

NC-CA tuân thủ các trường mở rộng của CRL theo quy định của cơ quan có thẩm quyền. Hiện tại NC-CA chưa bắt buộc áp dụng trường mở rộng CRL nào.

## Hồ sơ OCSP

Phiên bản

Chứng thư số OCSP Responder sử dụng trong Hệ thống được NC-CA ban hành theo chuẩn ITU-T X.509 v3 và các quy định của RFC 5280.

Hệ thống kiểm tra trạng thái các loại chứng thư sau theo chuẩn OCSP mô tả trong RFC2560:

* Chứng thư số cho cá nhân
* Chứng thư số cho tổ chức, doanh nghiệp

Trường cơ bản

Chứng thư số OCSP Responder bao gồm các trường sau:

|  |  |
| --- | --- |
| **Trường Giá trị** | **Ý nghĩa** |
| Serial Number | Giá trị là duy nhất đối với mỗi chứng thư số do NC-CA ban hành |
| Signature Algorithm | Định danh (OID) của thuật toán được sử dụng để kí lên chứng thư số |
| Issuer | NC-CA |
| Valid From | Thời điểm bắt đầu chứng thư số có hiệu lực, theo giờ Việt nam |
| Valid To | Thời điểm hết hiệu lực của chứng thư số, theo giờ Việt nam |
| Subject DN | Xem phần VII.1.4 |
| Subject Public key | Khóa công khai, được mã hóa phù hợp với RFC 5280 |
| Signature | Chữ kí số của NC-CA được mã hóa phù hợp với RFC 5280 |

Trường mở rộng

Chứng thư số OCSP Responder bao gồm các trường mở rộng sau:

|  |  |
| --- | --- |
| **Trường Giá trị** | **Ý nghĩa** |
| Basic Contraints (basicContraints) | Chứa thông tin xác định đây có phải là CA không và độ sâu lớn nhất của cấu trúc phân cấp chứng thư (certificate path) |
| Key Usage (keyUsage) | Mô tả mục đích sử dụng của khóa được lưu trong chứng thư |
| Subject Key Identifier (subjectKeyIdentifier) | Xác định các chứng thư chứa một khóa công khai cụ thể |
| Subject Alternative Name (subjectAltName) | Cho phép bổ sung thêm các định danh gắn với chủ thể của chứng thư được cấp phát |
| Extended Key Usage (extendedKeyUsage) | Đưa ra một hoặc nhiều các mục đích sử dụng của khóa bổ xung cho mục đích sử dụng xác định trong mục Key Usage |

KIỂM TOÁN MỨC TUÂN THỦ VÀ CÁC ĐÁNH GIÁ KHÁC

Việc kiểm toán kỹ thuật các hoạt động NC-CA được thực hiện định kỳ từ công ty cổ phần hỗ trợ doanh nghiệp và đầu tư HN hoặc theo yêu cầu từ Trung tâm Chứng thực điện tử quốc gia.

## Tần suất và các tình huống kiểm toán kỹ thuật

Kiểm toán kỹ thuật được thực hiện ít nhất một năm một lần, phí tổn thuộc về công ty cổ phần hỗ trợ doanh nghiệp và đầu tư HN.

## Đơn vị thực hiện kiểm toán kỹ thuật

Đơn vị thực hiện kiểm toán kỹ thuật NC-CA được chỉ định bởi công ty cổ phần hỗ trợ doanh nghiệp và đầu tư HN hoặc bởi Trung tâm Chứng thực điện tử quốc gia.

## Mối quan hệ của đơn vị kiểm toán kỹ thuật với NC-CA

Kiểm toán kỹ thuật được thực hiện bởi những đơn vị không phụ thuộc vào NC-CA.

## Các nội dung kiểm toán kỹ thuật

Các lĩnh vực được kiểm toán kỹ thuật bao gồm: hạ tầng hệ thống, các quy trình quản lý khóa, quy trình vận hành hệ thống và các nội dung khác theo yêu cầu của đơn vị kiểm toán kỹ thuật.

## Xử lý khi phát hiện sai sót

Sau khi có báo cáo kiểm toán kỹ thuật, NC-CA sẽ làm việc với đơn vị kiểm toán về những nội dung chưa phù hợp.

NC-CA sẽ nghiên cứu và đề ra và thực hiện phương án xử lý những nội dung chưa phù hợp trong thời gian thống nhất đơn vị tiến hành kiểm toán và có báo cáo Trung tâm Chứng thực điện tử quốc gia.

Dịch vụ của NC-CA sẽ bị ngừng trong các tình huống sau:

* Báo cáo kiểm toán kỹ thuật cho thấy có lỗi nghiêm trọng có thể ảnh hưởng ngay lập tức tới an ninh của hệ thống NC-CA.
* NC-CA thực hiện kế hoạch xử lý lỗi nhưng không có kết quả.

## Công bố kết quả kiểm toán kỹ thuật

Báo cáo kết quả kiểm toán kỹ thuật được NC-CA gửi Trung tâm Chứng thực điện tử quốc gia và nếu được phép sẽ công bố.

CÁC NỘI DUNG NGHIỆP VỤ VÀ PHÁP LÝ KHÁC

##  Phí

 Phí cấp phát, gia hạn, thay đổi khóa và thu hồi chứng thư số

- Phí cấp phát, gia hạn chứng thư số: Theo bảng giá trên hợp đồng

- Phí thay đổi khóa, thu hồi chứng thư số: Miễn phí

 Phí truy cập chứng thư số

Miễn phí

 Phí truy cập thông tin trạng thái thu hồi (Dịch vụ xác minh hiệu lực của chứng thư số)

Miễn phí

 Phí cho những dịch vụ khác như là thông tin về chính sách

NC-CA và RA, đại lý có thể thiết lập và tính một mức phí hợp lý cho dịch vụ khác.

 Phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số

\* Cơ sở pháp lý: Thông tư 305/2016/TT-BTC ngày 15/11/2016 quy định mức thu, chế độ thu, nộp, quản lý và sử dụng phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số.

- Mức thu phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số: 3.000 đồng/chữ ký số/tháng.

- Chứng thư số phát sinh hiệu lực hoạt động tại bất cứ thời điểm nào của tháng được tính là 01 (một) tháng sử dụng.

9.1.6. Chính sách hoàn phí

Bất kỳ các khoản phí nào cho việc đề nghị cấp chứng thư số mà không được phê chuẩn sẽ được hoàn trả.

##  Trách nhiệm tài chính

NC-CA thực hiện Ký quỹ tại một ngân hàng thương mại hoạt động tại Việt Nam không dưới 05 (năm) tỷ đồng để giải quyết các rủi ro và các khoản đền bù có thể xảy ra trong quá trình cung cấp dịch vụ do lỗi của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng và thanh toán chi phí tiếp nhận và duy trì cơ sở dữ liệu của doanh nghiệp trong trường hợp bị thu hồi giấy phép theo quy định của nhà nước.

 Bảo hiểm

NC-CA sẽ cung cấp đa dạng các gói bảo hiểm dịch vụ chứng thực chữ ký số, khách hàng có thể tùy chọn theo mục đích sử dụng.

 Trách nhiệm bồi thường thiệt hại cho thuê bao

NC-CA có trách nhiệm bồi thường thiệt hại cho thuê bao trong những trường hợp sau:

- Thiệt hại xảy ra khi NC-CA để lộ quá trình tạo khóa, lộ khóa bí mật trong quá trình chuyển giao, lưu trữ khóa bí mật và thông tin của thuê bao.

- Thiệt hại xảy ra là hậu quả của việc để lộ thông tin của thuê bao mà NC-CA có nghĩa vụ lưu trữ bí mật.

- Thiệt hại xảy ra là đưa lên chứng thư số những thông tin không chính xác so với những thông tin do thuê bao cung cấp.

- Thiệt hại xảy ra là hậu quả của việc không tuân thủ các quy định tại khoản 2, 3 0

- NC-CA có trách nhiệm bồi thường theo các mức bảo hiểm đã công bố.

 Trách nhiệm bồi thường của bên khác

(1). Bồi thường bởi bên vi phạm

Trong phạm vi của luật áp dụng, bên vi phạm bồi thường cho NC-CA và cho các bên liên quan trong các trường hợp:

• Xuyên tạc sự thật trong đơn đăng ký cấp chứng thư số.

• Vi phạm tiết lộ những tài liệu trên đơn xin cấp chứng thư số, nếu những thông tin sai lệch hoặc bỏ sót do sự cẩu thả hay do cố ý để đánh lừa bất kỳ tổ chức nào.

• Thiếu sót trong việc bảo vệ khóa riêng, hoặc trong những hành động cảnh báo cần thiết để chống lại việc tiết lộ, mất mát, sửa chữa hoặc sử dụng trái phép khóa riêng của chủ thể cuối cùng hoặc sử dụng tên của chủ thể cuối cùng (bao gồm, không giới hạn bởi tên thường dùng, hoặc địa chỉ email) xâm phạm quyền sở hữu trí tuệ của bên thứ ba.

(2). Bồi thường do bên nhận

Trong phạm vi của luật áp dụng, thỏa thuận bên nhận và các thỏa thuận khác yêu cầu bên nhận bồi thường cho NC-CA và cho các bên liên quan về

• Bên nhận thiếu sót trong việc thực hiện các nghĩa vụ của mình;

• Sự tin tưởng của bên nhận vào chứng thư số không phù hợp trong một số trường hợp; hoặc

• Bên nhận thiếu sót trong việc kiểm tra tình trạng của chứng thư số để xác định xem liệu chứng thư số đó đã hết hạn hay bị thu hồi hay chưa.

## Tính bí mật của thông tin nghiệp vụ

Phạm vi các thông tin bí mật

Những thông tin sau sẽ được coi là thông tin bí mật:

* Các thông tin được yêu cầu bởi pháp luật.
* Hồ sơ đăng ký cấp chứng thư số.
* Nhật ký của NC-CA.
* Báo cáo kiểm toán kỹ thuật của NC-CA.
* Kế hoạch đối phó với sự cố và kế hoạch khôi phục lại sau thảm họa của NC-CA.
* Phương pháp điều khiển hoạt động các thành phần NC-CA: phần cứng, phần mềm và quản trị của dịch vụ của NC-CA.

Những thông tin ngoài phạm vi thông tin bí mật

Các thông tin không được coi là bí mật:

* Chứng thư số, trạng thái thu hồi của chứng thư số và thông tin trạng thái khác, địa chỉ website của NC-CA trên mạng và các thông tin trên đó.
* Không được chỉ rõ trong phần IX.3.1.

Trách nhiệm bảo vệ các thông tin bí mật

NC-CA thực hiện các biện pháp đảm bảo an ninh cho các thông tin bí mật.

## Tính riêng tư của thông tin cá nhân

Kế hoạch bảo mật thông tin cá nhân

Chính sách bảo mật thông tin cá nhân được công ty cổ phần hỗ trợ doanh nghiệp và đầu tư HN thông qua và được công bố trên website của NC-CA và thông báo cho thuê bao khi tiến hành đăng ký chứng thư số.

Phạm vi các thông tin cá nhân

Mọi thông tin thuê bao không được công bố qua nội dung của chứng thư số, dịch vụ thư mục và CRL được coi là bí mật.

Những thông tin ngoài phạm vi thông tin cá nhân

Mọi thông tin được công bố trong một chứng thư số, dịch vụ thư mục và CRL được coi là không bí mật.

Trách nhiệm bảo vệ các thông tin bí mật

NC-CA thực hiện các biện pháp đảm bảo an ninh cho các thông tin bí mật của thuê bao, tuân theo yêu cầu của luật pháp.

Thông báo và sự đồng thuận sử dụng thông tin mật

Thông tin bí mật sẽ không được sử dụng mà không có sự cho phép của người sở hữu thông tin hoặc đại điện sở hữu thông tin đó, trừ những trường hợp được quy định trong quy chế này hoặc trong các thỏa thuận cụ thể.

Cung cấp thông tin theo yêu cầu của cơ quan pháp luật

NC-CA sẽ cung cấp thông tin bí mật nếu có yêu cầu của cơ quan pháp luật có thẩm quyền và tuân thủ theo quy định của pháp luật.

Các tình huống cung cấp thông tin khác

NC-CA không cung cấp thông tin cho các đối tượng nào khác ngoài đại diện có thẩm quyền của pháp luật.

## Quyền sở hữu trí tuệ

Quyền sở hữu những thông tin chứng thư số và thu hồi

NC-CA giữ mọi quyền sở hữu chứng thư số và thông tin thu hồi mà nó tạo ra.

NC-CA cho phép sử dụng thông tin thu hồi khi thực hiện chức năng của người nhận.

Quyền sở hữu quy chế chứng thực

NC-CA giữ mọi quyền sở hữu trí tuệ quy chế chứng thực này.

Quyền sở hữu tên

NC-CA là quyền sở hữu tên của công ty cổ phần hỗ trợ doanh nghiệp và đầu tư HN.

Quyền sở hữu khóa

Cặp khoá tương ứng với chứng thư số của NC-CA, RA, thuê bao được sở hữu bởi chính đối tượng là chủ thể của chứng thư số đó.

## Tuyên bố và cam kết

Tuyên bố và cam kết của NC-CA

NC-CA đảm bảo rằng:

* Không thay đổi thông tin đăng ký chứng thư số được cung cấp bởi đối tượng đăng ký.
* Không có lỗi trong quá trình duyệt và cấp phát chứng thư số.
* Chứng thư số do NC-CA ban hành đáp ứng các yêu cầu trong quy chế này.

Tuyên bố và cam kết của RA

RA đảm bảo rằng:

* Không thay đổi thông tin đăng ký chứng thư số được cung cấp bởi đối tượng đăng ký.
* Tuân thủ hợp đồng với NC-CA.
* Thực hiện nghĩa vụ Đại lý tại điều 35 Nghị định số 130/2018/NĐ-CP.

Tuyên bố và cam kết của thuê bao

Thuê bao đảm bảo rằng:

* Khi ký, thuê bao sử dụng khóa bí mật tương ứng với khóa công khai trong chứng thư số; tại thời điểm ký, thuê bao chấp nhận chứng thư số và chứng thư số đang có hiệu lực (không hết hạn hoặc bị thu hồi).
* Khóa bí mật của mình được bảo vệ và không cho người khác sử dụng.
* Mọi thông tin cung cấp bởi thuê bao là đúng.
* Sử dụng chứng thư số đúng mục đích của chứng thư số, phù hợp với quy định của pháp luật và quy chế chứng thực này.

NC-CA khuyến cáo cần phải lưu trữ chứng thư số trong các thiết bị lưu trữ chuyên dụng.

Thỏa thuận thuê bao có thể bao gồm thêm những điều khoản khác do NC-CA quy định.

Nếu thuê bao vi phạm các cam kết trên, thuê bao chịu hoàn toàn trách nhiệm và phải đền bù các thiệt hại gây ra theo quy định của pháp luật.

Tuyên bố và cam kết của người nhận

Người nhận chịu trách nhiệm về việc tìm hiểu các thông tin trong quy chế chứng thư số, trong thỏa thuận người nhận trước khi quyết định tin tưởng chứng thư số do NC-CA ban hành.

Người nhận phải chịu trách nhiệm cho những hành động của mình do không thực hiện theo các nội dung liên quan được quy định trong thỏa thuận người nhận hoặc quy chế chứng thực này.

Tuyên bố và cam kết của các đối tượng khác

Ngoài các cam kết do NC-CA quy định, RA, thuê bao và người nhận, không có tuyên bố và cam kết của đối tượng nào khác được NC-CA chấp nhận.

## Tuyên bố về sự đảm bảo

Tuyên bố về đảm bảo hệ thống 24/7

Hệ thống chứng thực cung cấp dịch vụ chứng thực chữ ký số NC-CA được đặt tại hệ thống Data Center của FPT và Viettel. Hệ thống NC-CA được thiết lập đảm bảo

* Hệ thống hoạt động 24/7.
* Hiệu năng cao
* Có phương án dự phòng đầy đủ trong trường hợp xảy ra thảm họa.

Tuyên bố đảm bảo tuân thủ quy định phát luật và tiêu chuẩn của Bộ Thông tin và Truyền thông

NC-CA đảm bảo tuân thủ các quy đinh của pháp luật về dịch vụ chứng thực chữ ký số.

NC-CA đảm bảo tuân thủ các tiêu chuẩn về dịch vụ chữ ký số mà Bộ Thông tin và Truyền thông đưa ra

##  Giới hạn về trách nhiệm

Trong giới hạn của luật pháp, hợp đồng thuê bao và người nhận có thể giới hạn khả năng trách nhiệm pháp lý của NC-CA. Việc giới hạn trách nhiệm pháp lý bao gồm cả việc loại bỏ các thiệt hại ngẫu nhiên, gián tiếp, hay những thiệt hại nghiêm trọng.

Trách nhiệm pháp lý của thuê bao và NC-CA sẽ được thiết lập trong *Hợp đồng dịch vụ*.

##  Bồi thường

### *Vấn đề bồi thường của thuê bao*

Khi pháp luật yêu cầu, thuê bao phải bồi thường cho NC-CA nếu xuất hiện:

- Những thông tin sai lệch hoặc xuyên tạc sự thật do thuê bao cung cấp trên dịch vụ chứng thư số;

- Lỗi của thuê bao để lộ những nhân tố, yếu tố liên quan đến dịch vụ chứng thư số, sự bỏ sót hay làm sai lệch do sự cẩu thả hay với mục đích lừa đảo;

- Lỗi của thuê bao trong việc bảo vệ khóa bí mật, sử dụng hệ thống tin cậy, hoặc không thực hiện các biện pháp phòng ngừa cần thiết để tránh gây hậu quả;

- Việc sử dụng tên của thuê bao (kể cả việc không giới hạn tên chung, tên miền, hoặc địa chỉ thư điện tử) vi phạm quyền sở hữu trí tuệ của một bên thứ ba.

Hợp đồng dịch vụ có thể có thêm các thỏa thuận khác.

### *Vấn đề bồi thường của người nhận*

Khi được pháp luật cho phép, NC-CA có quyền yêu cầu người nhận bồi thường thiệt hại trong các trường hợp:

* - Lỗi của người nhận trong việc thực thi nghĩa vụ với một bên đối tác;
* - Sự tin cậy của người nhận về một chứng thư số không được đáp ứng trong một số trường hợp;
* - Lỗi của người nhận trong việc kiểm tra trạng thái của chứng thư số để xác định chứng thư số đã hết hạn hay bị thu hồi.

Hợp đồng với người nhận sẽ bao gồm thêm một số nghĩa vụ khác.

##  Điều khoản và sự kết thúc

Thời hạn bắt đầu có hiệu lực

Quy chế chứng thư số này có hiệu lực khi được công bố trên website của NC-CA. Các nội dung bổ sung cho quy chế chứng thư số này có hiệu lực khi được công bố.

Thời hạn hết hiệu lực

Quy chế này được còn hiệu lực cho đến khi nó được thay thế bằng một phiên bản mới.

Ảnh hưởng của quy chế chứng thư số hết hiệu lực

Khi quy chế này hết hiệu lực, các điều khoản của nó vẫn được áp dụng cho các chứng thư số được ban hành trong thời hạn của quy chế này cho đến khi chứng thư số hết hạn hoặc bị thu hồi.

## Thông báo cho thuê bao và liên lạc với các bên có tham gia

Trừ khi được quy định rõ ràng, các thành viên NC-CA sẽ sử dụng các phương pháp liên lạc hợp lý, tùy thuộc mức độ nguy cấp về nội dung của thông tin cần liên lạc.

## Thay đổi Quy chế chứng thực

Thủ tục bổ sung

Quy chế này được bổ sung, sửa đổi bởi tổ chuyên gia do công ty cổ phần hỗ trợ doanh nghiệp và đầu tư HN phê chuẩn.

Nội dung sửa đổi sẽ thay thế các nội dung trong các điều khoản tương đương trong phiên bản quy chế chứng thực tương ứng và mọi tài liệu liên quan khác.

Nội dung của Quy chế chứng thực của NC-CA được Bộ Thông tin và truyền thông phê duyệt trước khi ban hành.

Cơ chế và thời hạn thông báo

Đối với các thay đổi không quan trọng như thay đổi URL, thông tin liên hệ, lỗi in ấn… NC-CA có quyền thay đổi quy chế mà không cần thông báo về sự thay đổi.

Trong trường hợp các thay đổi được phê duyệt có liên quan tới an ninh của hệ thống, NC-CA sẽ thực hiện sự thay đổi quy chế này lập tức, sau đó sẽ thông báo cho các tổ chức cá nhân có liên quan và Trung tâm Chứng thực điện tử quốc gia để được phê duyệt.

## Giải quyết các bất đồng , tranh chấp

Thực hiện theo quy định của công ty cổ phần hỗ trợ doanh nghiệp và đầu tư HN và trong hợp đồng cung cấp dịch vụ.

## Luật điều chỉnh

Pháp luật Việt Nam sẽ được sử dụng trong mọi trường hợp để xử lý tranh chấp liên quan đến các dịch vụ và chứng thư số do NC-CA cấp, kể cả trường hợp có liên quan đến các yếu tố nước ngoài.

## Tính tuân thủ với các luật pháp được áp dụng

Nếu có quy định trong quy chế này xung đột với quy định của các văn bản pháp luật, lúc này quy định của văn bản pháp luật sẽ có hiệu lực.

##  Điều khoản chung

Quy chế chứng thực này là thỏa thuận mà mọi thành viên của NC-CA phải tuân thủ.

Không có quy định nào cho phép chuyển nhượng quyền sử dụng chứng thư số. NC-CA không quy định các trường hợp chuyển nhượng khác.

Nếu như một số điều khoản trong quy chế chứng thực này không hợp pháp các điều khoản đó sẽ không có giá trị, nhưng không ảnh hưởng đến hiệu lực của các điều khoản khác.

##  Điều khoản khác

Không quy định.

TÀI LIỆU THAM CHIẾU

1. Luật Giao dịch điện tử số 51/2005/QH11 ngày 29 tháng 11 năm 2005;
2. Nghị định số 130/2018/NĐ-CP ngày 27 tháng 9 năm 2018 của Chính phủ quy định chi tiết thi hành Luật Giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số;
3. Thông tư 06/2015/TT-BTTTT của Bộ Thông tin và Truyền thông về danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và chứng thực chữ ký số.

1. <http://www.ietf.org/rfc/rfc3647.txt> (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework). Đây là chuẩn về Chính sách và Quy chế chứng thực, được Bộ Thông tin và Truyền thông chấp nhận tại [3].