



Công ty cổ phần dịch vụ T-van Hilo



CÔNG TY CỔ PHẦN DỊCH VỤ T_VAN HILO

Mã số thuế: 0106713804

QUY CHẾ CHỨNG THỰC



Hà Nội 2025

MỤC LỤC

1. GIỚI THIỆU:	8
1.1 Tổng quan:	8
1.2 Tên và dấu hiệu nhận diện tài liệu:	8
1.3 Các thành phần trong hệ thống dịch vụ chứng thực chữ ký số HILO-CA:	9
1.3.1 Tổ chức cung cấp dịch vụ chứng thực điện tử Quốc gia (Trung tâm Chứng thực điện tử Quốc gia):	10
1.3.2 Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng:	10
1.3.3 Thuê bao:	10
1.3.4 Bên tin tưởng:	10
1.3.5 Các bên khác:	10
1.4 Mục đích sử dụng chứng thư số Chữ ký số:	11
1.4.1 Các trường hợp sử dụng chứng thư Chữ ký số hợp lệ:	11
1.4.2 Các trường hợp không được sử dụng chứng thư Chữ ký số HILO-CA:	11
1.5 Quản lý Quy chế chứng thực:	11
1.5.1 Tổ chức quản lý Quy chế chứng thực:	11
1.5.2 Thông tin liên hệ:	11
1.5.3 Cơ quan, tổ chức đánh giá sự phù hợp của Quy chế chứng thực với Pháp luật:	12
1.5.4 Thủ tục phê duyệt, ban hành quy chế chứng thực:	12
1.6 Các định nghĩa và từ viết tắt:	12
2. TRÁCH NHIỆM LƯU TRỮ, CÔNG BỐ THÔNG TIN:	12
2.1 Lưu trữ thông tin:	12
2.1.1 Lưu trữ hồ sơ khách hàng:	13
2.1.2 Lưu trữ thông tin thuê bao:	13
2.2 Công bố thông tin chứng thư số:	14
2.3 Thời gian và tần suất công bố:	15
2.4 Kiểm soát truy nhập thông tin:	15
3. ĐỊNH DANH VÀ XÁC THỰC YÊU CẦU ĐỀ NGHỊ PHÁT HÀNH CHỨNG THƯ CHỮ KÝ SỐ:	16
3.1 Đặt tên trong chứng thư chữ ký số:	16
3.1.1 Các kiểu tên:	16
3.1.2 Cần tên có ý nghĩa:	16
3.1.3 Ấn danh hoặc bút danh:	17
3.1.4 Quy tắc diễn giải các hình thức tên khác nhau:	17
3.1.5 Tính duy nhất của tên:	17
3.1.6 Nhận diện, xác thực và vai trò của nhân hiệu:	18
3.2 Xác minh đề nghị phát hành chứng thư chữ ký số:	18
3.2.1 Phương thức chứng minh quyền sở hữu khóa bí mật:	18
3.2.2 Xác minh danh tính đối với tổ chức:	25
3.2.3 Xác minh danh tính đối với cá nhân:	26
3.2.4 Thông tin thuê bao không được xác minh:	27
3.2.5 Xác minh thẩm quyền:	27
3.2.6 Tiêu chí liên thông:	27
3.3 Xác minh đề nghị thay đổi khóa:	27
3.3.1 Xác minh danh tính và xác thực đối với yêu cầu thay đổi cặp khóa định kỳ:	28
3.3.2 Xác minh danh tính và xác thực đối với yêu cầu thay đổi cặp khóa sau khi thu hồi:	2
9	
3.4 Xác thực định danh cho yêu cầu thu hồi chứng thư số	29
3.4.1 Quy trình đề nghị thu hồi chứng thư chữ ký số:	29
3.4.2 Thủ tục xác minh đề nghị thu hồi chứng thư chữ ký số:	29
4. CÁC YÊU CẦU ĐỐI VỚI VÒNG ĐỜI CỦA CHỨNG THƯ CHỮ KÝ SỐ:	30
4.1 Yêu cầu đề nghị phát hành chứng thư chữ ký số	30

4.1.1	Đối tượng đề nghị phát hành chứng thư chữ ký số:	30
4.1.2	Trách nhiệm và quy trình đăng ký:	31
4.2	Xử lý yêu cầu đề nghị phát hành chứng thư chữ ký số:	33
4.2.1	Thực hiện chức năng xác minh danh tính và xác thực:	33
4.2.2	Phê duyệt hoặc từ chối hồ sơ đề nghị phát hành chứng thư chữ ký số:	33
4.2.3	Thời gian xử lý hồ sơ đề nghị phát hành chứng thư chữ ký số:	34
4.3	Phát hành chứng thư chữ ký số:	34
4.3.1	Quy trình phát hành chứng thư chữ ký số:	34
4.3.2	Thông báo việc phát hành chứng thư chữ ký số:	36
4.4	Xác nhận và công bố công khai chứng thư chữ ký số:	36
4.4.1	Xác nhận các thông tin trên chứng thư chữ ký số được cấp là chính xác:	36
4.4.2	Công bố chứng thư chữ ký số theo quy định:	37
4.4.3	Thông báo đến các đối tượng khác về việc phát hành chứng thư chữ ký số:	38
4.5	Sử dụng cặp khóa và chứng thư chữ ký số:	38
4.5.1	Cách sử dụng chứng thư chữ ký số và khóa bí mật của thuê bao:	38
4.5.2	Cách sử dụng khóa công khai và chứng thư chữ ký số bởi các bên tin tưởng:	39
4.6	Gia hạn chứng thư chữ ký số:	39
4.6.1	Các trường hợp được gia hạn chứng thư chữ ký số của thuê bao:	39
4.6.2	Đối tượng có thể yêu cầu gia hạn chứng thư chữ ký số:	40
4.6.3	Xử lý yêu cầu gia hạn chứng thư chữ ký số:	40
4.6.4	Thông báo cho thuê bao về việc gia hạn chứng thư chữ ký số:	40
4.6.5	Xác nhận đối với chứng thư chữ ký số được gia hạn:	40
4.6.6	Công bố chứng thư chữ ký số đã được gia hạn:	40
4.6.7	Thông báo chứng thư chữ ký số được gia hạn đến các đối tượng khác:	40
4.7	Thay đổi cặp khóa của thuê bao:	40
4.7.1	Các trường hợp được thay đổi cặp khóa:	40
4.7.2	Đối tượng được gửi yêu cầu thay đổi cặp khóa:	41
4.7.3	Xử lý yêu cầu thay đổi cặp khóa:	41
4.7.4	Thông báo cập nhật chứng thư chữ ký số sau khi thay đổi cặp khóa:	41
4.7.5	Xác nhận đối với chứng thư chữ ký số được cập nhật:	41
4.7.6	Công bố chứng thư chữ ký số được cập nhật sau khi thay đổi cặp khóa:	41
4.7.7	Thông báo chứng thư chữ ký số được cập nhật sau khi thay đổi cặp khóa đến các đối tượng khác:	42
4.8	Thay đổi thông tin chứng thư chữ ký số:	42
4.8.1	Các trường hợp được thay đổi thông tin chứng thư chữ ký số:	42
4.8.2	Đối tượng được gửi yêu cầu thay đổi thông tin chứng thư chữ ký số:	42
4.8.3	Xử lý yêu cầu thay đổi thông tin chứng thư chữ ký số:	42
4.8.4	Thông báo cập nhật cho thuê bao về việc sửa đổi chứng thư chữ ký số:	43
4.8.5	Xác nhận đối với chứng thư chữ ký số được cập nhật:	43
4.8.6	Công bố chứng thư chữ ký số được cập nhật sau khi thay đổi thông tin:	43
4.8.7	Thông báo chứng thư chữ ký số được cập nhật sau khi thay đổi thông tin đến các đối tượng khác:	43
4.9	Tạm dừng, phục hồi, thu hồi chứng thư chữ ký số:	43
4.9.1	Các trường hợp được phép tạm dừng chứng thư chữ ký số:	43
4.9.2	Đối tượng được phép yêu cầu tạm dừng chứng thư chữ ký số:	43
4.9.3	Quy trình, thủ tục tạm dừng chứng thư chữ ký số:	44
4.9.4	Thời hạn gia hạn yêu cầu tạm dừng chứng thư chữ ký số:	44
4.9.5	Thời gian phải xử lý yêu cầu tạm dừng chứng thư chữ ký số:	44
4.9.6	Yêu cầu kiểm tra trạng thái thu hồi chứng thư chữ ký số đối với các bên tin tưởng:	44
4.9.7	Tần suất công bố danh sách thu hồi chứng thư chữ ký số(CRL):	44
4.9.8	Độ trễ công bố CRL:	45
4.9.9	Kiểm tra trạng thái/ thu hồi chứng thư chữ ký số trực tuyến:	45
4.9.10	Yêu cầu kiểm tra trạng thái thu hồi chứng thư chữ ký số trực tuyến:	45

4.9.11 Các hình thức thông báo thu hồi khác:	45
4.9.12 Yêu cầu đặc biệt liên quan đến thay đổi cặp khóa:	45
4.9.13 Các trường hợp được phép tạm dừng, phục hồi chứng thư chữ ký số:	45
4.9.14 Đối tượng được phép yêu cầu tạm dừng chứng thư chữ ký số:	45
4.9.15 Quy trình, thủ tục yêu cầu tạm dừng, phục hồi chứng thư chữ ký số:	45
4.9.16 Giới hạn thời hạn tạm dừng, phục hồi chứng thư chữ ký số:	47
4.10 Kiểm tra trạng thái chứng thư chữ ký số:	47
4.10.1 Các hình thức kiểm tra trạng thái chứng thư chữ ký số của thuê bao:	47
4.10.2 Tính sẵn sàng của dịch vụ kiểm tra trạng thái chứng thư chữ ký số:	47
4.10.3 Các tính năng khác:	47
4.11 Chấm dứt dịch vụ của thuê bao:	47
4.11.1 Các trường hợp thuê bao chấm dứt dịch vụ:	47
4.11.2 Thủ tục chấm dứt dịch vụ:	48
4.12 Lưu trữ và phục hồi khóa:	48
4.12.1 Chính sách và thực tiễn việc lưu trữ và phục hồi khóa	48
4.12.2 Chính sách và thực tiễn việc mã hóa và phục hồi khóa phiên	42
5. KIỂM SOÁT, QUẢN LÝ VÀ VẬN HÀNH:	48
5.1 Kiểm soát an toàn, an ninh vật lý:	48
5.1.1 Vị trí đặt và xây dựng hệ thống:	48
5.1.2 Truy cập vật lý:	48
5.1.3 Điều hòa và nguồn điện:	49
5.1.4 Tiếp xúc với nước:	49
5.1.5 Phòng ngừa và bảo vệ chống cháy:	49
5.1.6 Phương tiện lưu trữ:	49
5.1.7 Xử lý rác:	49
5.1.8 Hệ thống dự phòng:	50
5.2 Kiểm soát quy trình:	50
5.2.1 Các vai trò đáng tin cậy:	50
5.2.2 Số lượng người cần thiết cho mỗi công việc:	51
5.2.3 Định danh và xác thực trong mỗi thành viên:	51
5.2.4 Vai trò, trách nhiệm của từng thành viên:	52
5.3 Kiểm soát nhân sự:	52
5.3.1 Kinh nghiệm, bằng cấp, chứng chỉ của đội ngũ nhân sự liên quan đến quản lý và vận hành hệ thống:	52
5.3.2 Quy trình kiểm tra lý lịch:	53
5.3.3 Yêu cầu về đào tạo cho cán bộ vận hành, quản lý hệ thống:	53
5.3.4 Tần suất và yêu cầu đào tạo lại:	54
5.3.5 Tần suất và trình tự luân chuyển công việc:	54
5.3.6 Các hình thức xử lý đối với hành động không được phép:	54
5.3.7 Yêu cầu đối với nhà thầu độc lập:	55
5.3.8 Cung cấp tài liệu cho nhân viên:	55
5.4 Các quy trình ghi nhật ký hệ thống:	55
5.4.1 Các loại sự kiện được ghi lại:	55
5.4.2 Tần suất xử lý nhật ký hệ thống:	56
5.4.3 Thời gian lưu trữ nhật ký hệ thống:	56
5.4.4 Bảo vệ nhật ký hệ thống:	56
5.4.5 Quy trình sao lưu nhật ký hệ thống:	57
5.4.6 Hệ thống thu thập nhật ký hệ thống:	57
5.4.7 Thông báo cho đối tượng gây ra sự kiện:	57
5.4.8 Đánh giá lỗ hổng bảo mật:	57
5.5 Lưu trữ các bản ghi:	57
5.5.1 Các loại bản ghi được lưu trữ:	57
5.5.2 Thời hạn lưu trữ bản ghi:	58
5.5.3 Bảo vệ bản ghi lưu trữ:	58

5.5.4	Quy trình sao lưu bản ghi:	58
5.5.5	Yêu cầu về gắn dấu thời gian cho bản ghi:	58
5.5.6	Hệ thống thu thập bản ghi:	58
5.5.7	Quy trình truy cập và xác minh thông tin bản ghi:	58
5.6	Thay đổi cặp khóa:	58
5.7	Xử lý sự cố, thảm họa và phục hồi:	59
5.7.1	Quy trình xử lý sự cố và thảm họa:	59
5.7.2	Sự cố về tài nguyên máy tính, phần mềm và dữ liệu:	59
5.7.3	Quy trình xử lý khóa bí mật bị xâm phạm:	59
5.7.4	Khả năng phục hồi hoạt động sau thảm họa:	60
5.8	Dừng hoạt động cung cấp dịch vụ:	61
6.	ĐẢM BẢO AN TOÀN AN NINH VỀ KỸ THUẬT:	61
6.1	Tạo và phân phối khóa:	61
6.1.1	Cách thức tạo cặp khóa:	61
6.1.2	Chuyển giao khóa bí mật:	62
6.1.3	Chuyển giao khóa công khai cho tổ chức phát hành chứng thư chữ ký số:	62
6.1.4	Chuyển giao khóa công khai của tổ chức phát hành chứng thư chữ ký số cho bên tin tưởng:	62
6.1.5	Kích thước khóa:	62
6.1.6	Tạo các tham số cho khóa công khai và kiểm tra chất lượng:	62
6.1.7	Mục đích sử dụng khóa:	63
6.2	Kiểm soát và bảo vệ khóa bí mật, mô-đun mật mã:	63
6.2.1	Tiêu chuẩn và kiểm soát đối với mô-đun mật mã:	63
6.2.2	Kiểm soát đa bên đối với khóa bí mật(n out of m):	63
6.2.3	Chuyển giao khóa bí mật:	63
6.2.4	Dự phòng khóa bí mật:	64
6.2.5	Lưu trữ khóa bí mật:	64
6.2.6	Chuyển khóa bí mật vào hoặc ra khỏi Mô-đun mật mã:	64
6.2.7	Lưu trữ khóa bí mật trên Mô-đun mật mã:	64
6.2.8	Phương thức kích hoạt khóa bí mật:	64
6.2.9	Phương pháp vô hiệu hóa khóa bí mật:	64
6.2.10	Phương pháp hủy khóa bí mật:	65
6.2.11	Đánh giá Mô-đun mật mã:	65
6.3	Các vấn đề khác liên quan đến việc quản lý cặp khóa:	65
6.3.1	Lưu trữ khóa công khai:	65
6.3.2	Thời hạn sử dụng chứng thư chữ ký số và thời hạn sử dụng cặp khóa:	65
6.4	Kích hoạt dữ liệu:	65
6.4.1	Khởi tạo và cài đặt dữ liệu kích hoạt:	65
6.4.2	Bảo vệ dữ liệu kích hoạt:	66
6.4.3	Các khía cạnh khác của dữ liệu kích hoạt:	66
6.5	Kiểm soát an ninh máy tính:	66
6.5.1	Các yêu cầu kỹ thuật cụ thể về an ninh máy tính:	66
6.5.2	Định kỳ đánh giá an ninh hệ thống máy tính:	67
6.6	Kiểm soát vòng đời kỹ thuật:	67
6.6.1	Kiểm soát phát triển hệ thống:	67
6.6.2	Kiểm soát quản lý an ninh:	67
6.6.3	Kiểm soát vòng đời hệ thống:	67
6.7	Giám sát an ninh mạng hệ thống mạng:	67
6.8	Dấu thời gian:	67
7.	ĐỊNH DẠNG CHỨNG THƯ CHỮ KÝ SỐ, DANH SÁCH THU HỒI CHỨNG THƯ CHỮ KÝ SỐ (CRL), GIAO THỨC KIỂM TRA TRẠNG THÁI CHỨNG THƯ CHỮ KÝ SỐ TRỰC TUYẾN (OCSP):	67
7.1	Định dạng của chứng thư số:	68
7.1.1	Phiên bản:	68

7.1.2	Các trường mở rộng:	68
7.1.3	Định danh thuật toán:	69
7.1.4	Định dạng tên:	69
7.1.5	Các ràng buộc, hạn chế về tên:	69
7.1.6	Định danh quy chế chứng thực:	70
7.1.7	Sử dụng trường mở rộng Policy Constraint:	70
7.1.8	Củ pháp và ngữ nghĩa trong quy chế chứng thực:	70
7.1.9	Xử lý ngữ nghĩa trong trường mở rộng quan trọng Certificate Policies:	70
7.2	Định dạng danh sách thu hồi chứng thư chữ ký số (CRL):	70
7.2.1	Số phiên bản của CRL:	71
7.2.2	CRL và phần mở rộng đầu vào CRL:	71
7.3	Định dạng giao thức kiểm tra trạng thái chứng thư chữ ký số trực tuyến (OCSP):	71
7.3.1	Số phiên bản của OCSP:	71
7.3.2	Phần mở rộng OCSP:	71
8.	KIỂM ĐỊNH TÍNH TUÂN THỦ VÀ CÁC ĐÁNH GIÁ KHÁC:	71
8.1	Tần suất và các tình huống kiểm tra kỹ thuật:	71
8.2	Danh tính và khả năng của đơn vị, người kiểm tra:	71
8.3	Tính độc lập của bên đánh giá đối với tổ chức được đánh giá:	71
8.4	Xử lý khi phát hiện sai sót:	72
8.5	Công bố kết quả kiểm tra kỹ thuật:	72
8.6	Tần suất và các trường hợp đánh giá:	72
9.	CÁC NỘI DUNG NGHIỆP VỤ VÀ PHÁP LÝ KHÁC:	72
9.1	Phí/Giá:	72
9.1.1	Phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư chữ ký số:	72
9.1.2	Giá:	73
9.1.3	Các loại chi phí khác:	73
9.2	Trách nhiệm tài chính:	73
9.2.1	Phạm vi bảo hiểm:	73
9.2.2	Các tài sản khác:	74
9.2.3	Phạm vi bảo hiểm hoặc bảo hành cho người dùng cuối:	74
9.3	Bảo mật các thông tin nghiệp vụ:	74
9.3.1	Phạm vi thông tin nghiệp vụ cần được bảo mật:	74
9.3.2	Thông tin nằm ngoài phạm vi bảo mật:	75
9.3.3	Trách nhiệm bảo mật thông tin nghiệp vụ:	75
9.4	Bảo vệ dữ liệu cá nhân:	75
9.4.1	Biện pháp bảo vệ dữ liệu cá nhân:	75
9.4.2	Phạm vi bảo vệ dữ liệu cá nhân:	75
9.4.3	Những thông tin cá nhân ngoài phạm vi bảo vệ:	76
9.4.4	Trách nhiệm bảo vệ dữ liệu cá nhân:	76
9.4.5	Thông báo và cho phép sử dụng dữ liệu cá nhân:	76
9.4.6	Cung cấp thông tin riêng tư theo yêu cầu của Cơ quan quản lý:	76
9.4.7	Các tình huống cung cấp thông tin khác:	77
9.5	Quyền sở hữu trí tuệ:	77
9.5.1	Quyền sở hữu trong chứng thư số và thông tin thu hồi chứng thư chữ ký số:	77
9.5.2	Quyền sở hữu trong CPS:	78
9.5.3	Quyền sở hữu tên:	78
9.5.4	Quyền sở hữu khóa và các tài liệu của khóa:	78
9.6	Tuyên bố và cam kết:	78
9.6.1	Tuyên bố và cam kết của tổ chức phát hành chứng thư chữ ký số:	78
9.6.2	Tuyên bố và cam kết của Thuê bao:	78
9.6.3	Tuyên bố và cam kết của bên tin tưởng:	79
9.6.4	Tuyên bố và cam kết của các bên liên quan khác:	79
9.7	Từ chối bảo lãnh:	80

9.8	Giới hạn trách nhiệm:	80
9.9	Bồi thường thiệt hại:	80
9.9.1	Vấn đề bồi thường của thuê bao:	80
9.9.2	Vấn đề bồi thường của người nhận:	80
9.10	Hiệu lực của CPS:	81
9.10.1	Thời hạn của CPS:	81
9.10.2	Chấm dứt hiệu lực và các tồn tại:	81
9.10.3	Ảnh hưởng của việc chấm dứt hiệu lực:	81
9.11	Thông báo và trao đổi thông tin với các bên tham gia:	82
9.12	Bổ sung và sửa đổi:	82
9.12.1	Quy trình sửa đổi:	82
9.12.2	Cơ chế và thời hạn thông báo:	82
9.12.3	Các trường hợp cần thay đổi OID (Object identifier-mã định danh đối tượng):	83
9.13	Thủ tục giải quyết khiếu nại:	83
9.13.1	Tranh chấp giữa HILO-CA, đối tác và thuê bao:	83
9.13.2	Tranh chấp với thuê bao hay người nhận:	83
9.14	Hệ thống căn cứ pháp lý:	83
9.15	Tuân thủ quy định pháp luật hiện hành:	84
9.16	Các điều khoản chung:	84
9.16.1	Thỏa thuận toàn bộ:	84
9.16.2	Chuyển nhượng:	84
9.16.3	Tính độc lập của các điều khoản:	84
9.16.4	Sự thực thi (quyền ủy nhiệm và quyền khước từ):	84
9.16.5	Sự kiện bất khả kháng:	84
9.17	Các điều khoản khác:	85

1. GIỚI THIỆU:

1.1 Tổng quan:

HILO-CA là tên gọi dịch vụ chứng thực chữ ký số công cộng do Công ty cổ phần Dịch vụ T-Van Hilo cung cấp theo giấy phép số 690 do Bộ Thông tin và Truyền thông (Nay là Bộ Khoa học và Công nghệ) cấp ngày 25 tháng 10 năm 2021. Các quy định về chính sách chứng thư chữ ký số của HILO-CA được trình bày trong tài liệu này gồm có các quy trình quản lý cấp phát, gia hạn, thu hồi, tạm dừng, khôi phục, hủy bỏ chứng thư chữ ký số cho các thuê bao là cá nhân, tổ chức doanh nghiệp...

Bản quy chế chứng thực mô tả các thủ tục và cơ chế thực thi của nhà cung cấp chứng thư chữ ký số của hệ thống HILO-CA. Quy chế chứng thực mô tả các điều khoản và điều kiện thực hiện của nó nhằm cung cấp tới các cơ quan quản lý cũng như người sử dụng những mô tả rõ ràng về các dịch vụ của hệ thống và các điều kiện để sử dụng chúng. Ngoài ra, nó cũng đưa ra những đảm bảo về mặt an toàn bảo mật và an toàn thông tin của hệ thống HILO-CA và các dịch vụ chứng thực chữ ký số cung cấp cho khách hàng.

Hệ thống HILO-CA được tuân thủ theo luật giao dịch điện tử số 51/2005/QH11 Ngày 29 tháng 11 năm 2005; Luật giao dịch điện tử số 20/2023/QH15 ngày 22 tháng 06 năm 2023; Nghị định số 23/2025/NĐ-CP ngày 21 tháng 02 năm 2025 của Chính phủ quy định về chữ ký điện tử và dịch vụ tin cậy; Thông tư số 31/2020/TT-BTTTT ngày 30 tháng 10 năm 2020; Thông tư 19/2022/TT-BTC quy định về mức thu, chế độ thu, nộp, quản lý và sử dụng phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư chữ ký số; Nghị định số 13/2023/NĐ-CP của Chính phủ: Bảo vệ dữ liệu cá nhân và các quy định pháp luật hiện hành khác liên quan lĩnh vực chữ ký số.

1.2 Tên và dấu hiệu nhận diện tài liệu:

Văn bản này là một bộ quy chế chứng thực (Certificate Practices Statement - CPS) tuyên bố về mặt nguyên tắc các chính sách quản trị của HILO-CA trong quá trình cung cấp dịch vụ chứng thực chữ ký số công cộng.

CPS này là một chính sách quan trọng trong quá trình cung cấp dịch vụ chứng thực chữ ký số, đưa ra các yêu cầu về kinh doanh, pháp lý và kỹ thuật cho quá trình chấp thuận, cấp phát, quản lý, sử dụng, thu hồi và cấp lại chứng thư chữ ký số trong hệ thống HILO-CA. Các yêu cầu của CPS có nhiệm vụ đảm bảo tính bảo mật và toàn vẹn

cho dịch vụ HILO-CA, được áp dụng và bắt buộc tuân thủ đối với mọi thành phần tham gia dịch vụ chứng thực chữ ký số HILO-CA.

CPS này không phải là thỏa thuận về mặt pháp lý giữa HILO-CA với thuê bao cũng như các thành phần khác tham gia dịch vụ HILO-CA.

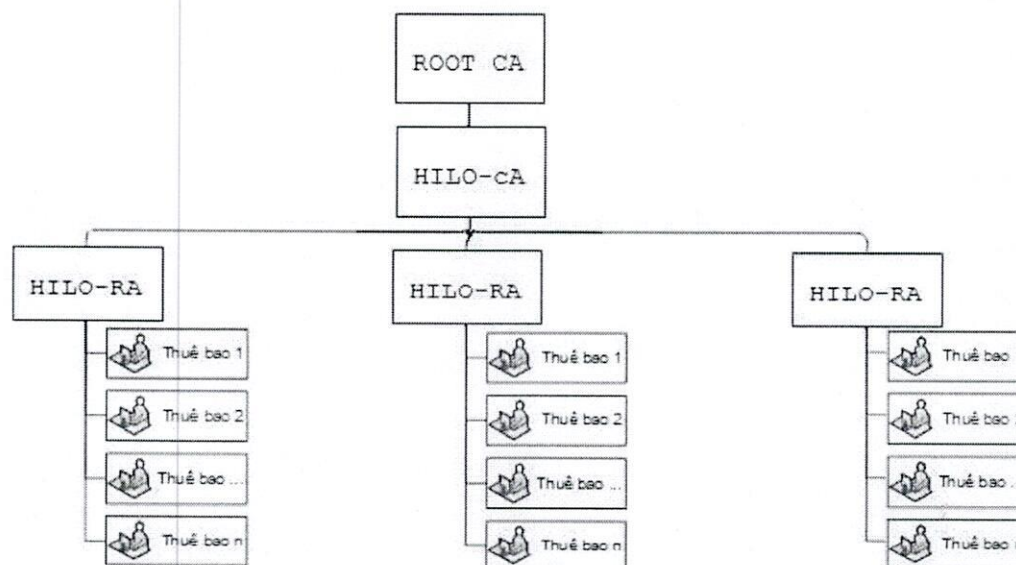
Mục tiêu của văn bản này là:

- HILO-CA với tư cách là nhà cung cấp dịch vụ chứng thực chữ ký số công cộng hoạt động trên cơ sở Quy chế chứng thực và tuân thủ theo các yêu cầu trong CPS này;
- Cung cấp cho người sử dụng dịch vụ HILO-CA các quy trình liên quan đến cấp phát, quản lý, sử dụng, thu hồi và cấp lại chứng thư chữ ký số trong hệ thống HILO-CA cũng như trách nhiệm của họ trong khi tham gia vào các quá trình này;
- Cung cấp thông tin cho bên tin tưởng về mức độ bảo đảm của các chứng thư chữ ký số mà HILO-CA cung cấp cho người sử dụng.

CPS này tuân theo luật pháp Việt Nam cũng như các chính sách, quy chế liên quan đến dịch vụ chứng thực chữ ký số công cộng được ban hành bởi Bộ Khoa học và Công nghệ cũng như các cơ quan nhà nước có thẩm quyền liên quan.

CPS này được xây dựng tuân theo tiêu chuẩn RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework).

1.3 Các thành phần trong hệ thống dịch vụ chứng thực chữ ký số HILO-CA:



Hình 1 – Sơ đồ tổ chức hệ thống HILO-CA

Hệ thống HILO-CA hoạt động có các thành phần tham gia gồm:

1.3.1 Tổ chức cung cấp dịch vụ chứng thực điện tử Quốc gia (Trung tâm Chứng thực điện tử Quốc gia):

Hệ thống dịch vụ chứng thực chữ ký số Quốc gia do Bộ Khoa học và Công nghệ quản lý là hệ thống RootCA Quốc gia (ROOT-CA).

1.3.2 Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng:

Hệ thống HILO-CA được tổ chức theo quy định của pháp luật Việt Nam, trực thuộc ROOT-CA (Trung tâm Chứng thực điện tử Quốc gia) do Bộ Khoa học và Công nghệ quản lý. HILO-CA được Bộ Khoa học và Công nghệ cấp phép cung cấp dịch vụ chứng thực chữ ký số công cộng, do đó có quyền cấp chứng thư chữ ký số cho các tổ chức, doanh nghiệp, cá nhân (đủ điều kiện theo quy định của pháp luật và CPS này), có yêu cầu cấp chứng thư chữ ký số.

1.3.3 Thuê bao:

Là tổ chức, cá nhân (đủ điều kiện theo quy định của pháp luật và CPS này) được HILO-CA cấp chứng thư chữ ký số.

1.3.4 Bên tin tưởng:

HILO-RA (registration authority) là tổ chức được CA tin cậy, uỷ quyền tiếp nhận yêu cầu cung cấp dịch vụ và xác thực thông tin của thuê bao nhằm đảm bảo tính chính xác các thông tin trong chứng thư chữ ký số của thuê bao trên toàn hệ thống. HILO-RA là toàn bộ các chi nhánh trên toàn quốc và đối tác của HILO-CA có khả năng kiểm tra, xác thực định danh các thuê bao. Nhiệm vụ của HILO-RA là gồm

- Tiếp nhận yêu cầu cấp chứng thư chữ ký số và báo cho CA thông qua hệ thống thiết bị (phần cứng, phần mềm) và người vận hành hệ thống đó;
- Xác thực thông tin thuê bao theo yêu cầu quy định tại CPS này nhằm đảm bảo tính chính xác các thông tin trong chứng thư chữ ký số trên toàn hệ thống.

1.3.5 Các bên khác:

Các tổ chức, cá nhân sử dụng các chức năng của hệ thống HILO-CA để giải mã/xác thực thông tin nhận được từ thuê bao của HILO-CA.

1.4 Mục đích sử dụng chứng thư số Chữ ký số:

1.4.1 Các trường hợp sử dụng chứng thư Chữ ký số hợp lệ:

Chứng thư chữ ký số HILO-CA được cấp bởi RootCA quốc gia với mục đích sử dụng chính như sau: digitalSignature, nonrepudiation, keyAgreement, dataEncipherment và keyEncipherment (các trường trong Key Usage của chứng thư chữ ký số).

Chứng thư chữ ký số HILO-CA được sử dụng để ký phát hành chứng thư chữ ký số cho thuê bao, các danh sách chứng thư chữ ký số thu hồi CRLs của HILO-CA, chứng thư chữ ký số cho hệ thống kiểm tra chứng thư chữ ký số trực tuyến OCSP; để xác thực các chứng thư chữ ký số do HILO-CA cấp và xác thực dữ liệu đã ký số.

Chứng thư được cấp cho cá nhân: chứng thư được sử dụng với mục đích cá nhân, xác định danh tính. Phục vụ ký số, xác thực tài liệu điện tử, xác thực đăng nhập, SSL, mail...

Chứng thư được cấp cho tổ chức: chứng thư được cấp cho một tổ chức, doanh nghiệp. Chứng thư chữ ký số cho thiết bị Usbtoken, HSM, SSL server, mail server...

Chứng thư chữ ký số CodeSigning.

Tất cả chứng thư chữ ký số đều phải sử dụng theo quy định của pháp luật và CPS này.

1.4.2 Các trường hợp không được sử dụng chứng thư Chữ ký số:

Sử dụng chứng thư chữ ký số sai mục đích, sử dụng để thực hiện các hành vi vi phạm pháp luật sẽ bị cấm.

1.5 Quản lý Quy chế chứng thực:

1.5.1 Tổ chức quản lý Quy chế chứng thực:

Công ty cổ phần Dịch vụ T-Van Hilo là đơn vị soạn thảo, cập nhật CPS này.

CPS này có thể được tải tại trên <https://HILO-CA.vn/tai-lieu/>

1.5.2 Thông tin liên hệ:

Công ty cổ phần Dịch vụ T-Van Hilo.

Địa chỉ: Số 18 Đoàn Trần Nghiệp, Phường Hai Bà Trưng, TP Hà Nội.

Văn phòng giao dịch: Số 6 ngõ 95 Chùa Bộc, Phường Kim Liên, TP.Hà Nội.

Điện thoại: 1900 29 29 62

Email: info@hilo.com.vn

1.5.3 Cơ quan, tổ chức đánh giá sự phù hợp của Quy chế chứng thực với Pháp luật:

Bộ Khoa học và Công nghệ (Trung tâm chứng thực điện tử quốc gia – RootCA) là cơ quan có thẩm quyền quyết định tính hợp pháp của quy chế này.

1.5.4 Thủ tục phê duyệt, ban hành quy chế chứng thực:

Trong quá trình hoạt động, khi có thay đổi nội dung trong quy chế chứng thực, HILO-CA sẽ báo cáo và được sự đồng ý của Bộ Khoa học và Công nghệ (Trung tâm chứng thực điện tử quốc gia – RootCA) chấp nhận.

Các thay đổi phải được thể hiện bằng văn bản dưới dạng một tài liệu chứa các sửa đổi mẫu của CPS hay các thông tin về quá trình cập nhật.

Tất cả những phiên bản đã sửa đổi hoặc cập nhật thông tin được công bố tại đại chỉ <https://HILO-CA.vn/tai-lieu/>

1.6 Các định nghĩa và từ viết tắt:

Chi tiết trong Phụ lục.

2. TRÁCH NHIỆM LƯU TRỮ, CÔNG BỐ THÔNG TIN:

2.1 Lưu trữ thông tin:

HILO-CA thực hiện lưu trữ và sử dụng thông tin của thuê bao một cách bí mật, an toàn, chính xác, đầy đủ, kịp thời và chỉ sử dụng thông tin này cho các mục đích liên quan đến việc cung cấp dịch vụ chứng thực chữ ký điện tử, cấp và quản lý chứng thư chữ ký số.

HILO-CA có trách nhiệm:

2.1.1 Lưu trữ thông tin thuê bao và chứng thư chữ ký số:

- Lưu trữ toàn bộ thông tin thuê bao trong suốt thời gian chứng thư chữ ký số còn hiệu lực và tối thiểu 05 năm kể từ khi chứng thư chữ ký số hết hiệu lực.
- Lưu trữ danh sách các chứng thư chữ ký số còn hiệu lực, tạm dừng, hết hiệu lực; cho phép người sử dụng Internet tra cứu trực tuyến 24/7.
- Lưu trữ đầy đủ các tài liệu hướng dẫn người dùng và các tài liệu liên quan khác tại địa chỉ: <http://HILO-CA.vn/tai-lieu/>.

2.1.1 Lưu trữ hồ sơ khách hàng:

a. Hồ sơ giấy:

- Bao gồm: Phiếu đăng ký cấp chứng thư chữ ký số;
- 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 hoặc giấy chứng nhận đăng ký hộ kinh doanh;
- Thẻ căn cước công dân hoặc thẻ căn cước hoặc căn cước điện tử hoặc giấy chứng nhận căn cước hoặc tài khoản định danh điện tử mức độ 2(VNEID) hoặc hộ chiếu còn thời hạn; thị thực nhập cảnh còn thời hạn hoặc giấy tờ chứng minh được miễn thị thực nhập cảnh (đối với cá nhân là người nước ngoài);
- Giấy xác nhận thông tin khách hàng, Giấy ủy quyền/bổ nhiệm và các giấy tờ liên quan.
- Hồ sơ bản cứng được chỉnh lý, đánh số, lưu tại tủ riêng trong kho lưu trữ của bộ phận văn thư.
- Hồ sơ được scan và lưu trữ trên **RA Server** để phục vụ tra cứu, tìm kiếm nhanh chóng.

b. Hồ sơ điện tử:

- o Hồ sơ bản điện tử được ký số bằng chứng thư chữ ký số hợp lệ, còn hiệu lực của tổ chức/cá nhân.
- o Hồ sơ điện tử được lưu trữ trên **RA Server**, phục vụ tra cứu và khai thác thuận tiện.
- o HILO-CA khuyến khích khách hàng sử dụng hồ sơ điện tử để tận dụng lợi ích pháp lý và sự tiện lợi của Chứng thư chữ ký số.

2.1.2 Lưu trữ thông tin thuê bao:

Thông tin thuê bao sau khi được thẩm định sẽ được lưu trữ gồm:

- **Đối với tổ chức đề nghị cấp Chứng thư chữ ký số:**
 - o Tên tổ chức;
 - o Mã số thuế/mã số tổ chức/mã ngân sách;
 - o Địa chỉ đăng ký kinh doanh;

- Email;
- Số điện thoại;
- Thông tin website/tên miền (nếu sử dụng chứng thư SSL);
- Thông tin người đại diện pháp luật;
- Thông tin liên hệ khác.
- **Đối với cá nhân đại diện tổ chức:**
 - Họ và tên;
 - Thông tin tổ chức;
 - CC/CCCD/Hộ chiếu/Số chứng thực cá nhân;
 - Địa chỉ theo giấy tờ tùy thân;
 - Số điện thoại;
 - Email;
 - Thông tin sở hữu tên miền (nếu sử dụng chứng thư SSL).
- **Đối với cá nhân:**
 - Họ và tên;
 - CC/CCCD/Hộ chiếu/Số chứng thực cá nhân;
 - Địa chỉ theo giấy tờ tùy thân;
 - Số điện thoại;
 - Email;
 - Thông tin sở hữu tên miền (nếu sử dụng chứng thư SSL).

Lưu trữ dữ liệu liên quan đến giấy phép:

Toàn bộ thông tin, dữ liệu liên quan đến việc tạm đình chỉ hoặc thu hồi giấy phép, cũng như cơ sở dữ liệu về thuê bao và chứng thư chữ ký số, được lưu trữ ít nhất 05 năm kể từ khi giấy phép bị đình chỉ hoặc thu hồi.

2.2 Công bố thông tin chứng thư số:

Khi bàn giao chứng thư chữ ký số cho khách hàng, HILO-CA yêu cầu khách hàng ký giấy xác nhận thông tin thuê bao trên chứng thư chữ ký số là chính xác. Ngoài ra, thuê bao có thể xác nhận tính chính xác thông tin thuê bao bằng phương thức điện tử

trên giao diện phần mềm token manager service hoặc tại webportal của HILO thông qua đường dẫn liên kết tại email HILO gửi cho thuê bao.

Sau khi thuê bao xác nhận tính chính xác thông tin thuê bao thì chứng thư chữ ký số của sẽ được công bố rộng rãi.

HILO-CA duy trì và đảm bảo hoạt động của kho lưu trữ cho phép thuê bao và các thành phần tham gia dịch vụ HILO-CA khác truy xuất nhằm xác định trạng thái chứng thư chữ ký số cũng như danh sách các chứng thư chữ ký số bị tạm ngừng, thu hồi.

Các thông tin thường xuyên được HILO-CA cập nhật và công bố gồm có:

- Các chứng thư chữ ký số do HILO-CA cấp;
- CRL do HILO-CA quản lý;
- Tất cả các phiên bản cũ và hiện tại của CPS;
- Mẫu Hợp đồng dịch vụ giữa HILO-CA với thuê bao.
- Tài liệu hướng dẫn tra cứu thông tin dành cho thuê bao.

Nhằm đảm bảo tính công khai, CPS và các tài liệu khác được HILO-CA duy trì lưu trữ trực tuyến tại địa chỉ <https://HILO-CA.vn/tai-lieu/>

2.3 Thời gian và tần suất công bố:

- Quy chế chứng thực: được công bố, cập nhật kịp thời theo quy định tại mục 9.12 và khi có sửa đổi, bổ sung.
- Thỏa thuận thuê bao, thỏa thuận với người nhận chứng thư chữ ký số: được công bố, cập nhật khi có thay đổi, bảo đảm tính đầy đủ, chính xác.
- Chứng thư chữ ký số: được công bố ngay sau khi được ban hành và có xác nhận của thuê bao, chậm nhất không quá 24 giờ kể từ thời điểm phát hành.
- Trạng thái chứng thư chữ ký số: được công bố ngay lập tức trên OCSP Responder và duy trì liên tục 24 giờ trong ngày, 7 ngày trong tuần.
- Danh sách chứng thư chữ ký số bị thu hồi (CRL): được công bố, cập nhật hằng ngày và bảo đảm khả năng truy cập liên tục.

2.4 Kiểm soát truy nhập thông tin:

CRL, CPS được công bố công khai nhưng không cho phép sửa đổi hoặc thay thế tại địa chỉ <https://HILO-CA.vn/tai-lieu/>

Cập nhật CRL được thực hiện tự động bởi hệ thống HILO-CA;

Mọi thay đổi của CPS chỉ được phép thực hiện bởi cấp có thẩm quyền của HILO-CA sau khi được phê duyệt bằng văn bản của Bộ Khoa học và Công nghệ (Trung tâm chứng thực điện tử quốc gia – RootCA).

3. ĐỊNH DANH VÀ XÁC THỰC YÊU CẦU ĐỀ NGHỊ PHÁT HÀNH CHỨNG THƯ CHỮ KÝ SỐ:

3.1 Đặt tên trong chứng thư chữ ký số:

3.1.1 Các kiểu tên:

HILO-CA cung cấp các chứng thư chữ ký số được phân loại theo:

- Chứng thư chữ ký số tổ chức;
- Chứng thư chữ ký số cá nhân;
- Chứng thư chữ ký số cho cá nhân thuộc tổ chức;
- Chứng thư chữ ký số SSL (dùng cho máy chủ/website).

Mỗi chứng thư chữ ký số do HILO-CA phát hành đều chứa một tên phân biệt (Distinguished Name – DN), dùng để nhận dạng và phân biệt với các chứng thư chữ ký số khác, tuân thủ chuẩn X.501. DN được thể hiện trong các trường Issuer và Subject của chứng thư chữ ký số.

3.1.2 Cần tên có ý nghĩa:

Các thuộc tính (attributes) trong một DN mà HILO-CA sử dụng được mô tả chi tiết trong bảng dưới đây:

Thuộc tính	Giá trị
Quốc gia (C)	Hai chữ cái chỉ tên quốc gia theo ISO, Việt Nam được ký hiệu là “VN”
Tổ chức (O)	Tên tổ chức, cá nhân được cấp chứng thư chữ ký số hoặc tên miền đối với chứng thư chữ ký số được cấp cho tên miền
Bộ phận tổ chức (OU)	Tên đơn vị nằm trong tổ chức.
Tỉnh/Thành Phố (S)	Tên Tỉnh, Thành phố là nơi cư trú hoặc đặt trụ sở của thuê bao

Tên của thuê bao (CN)	Các loại giá trị của thuộc tính này: - Tên tổ chức - Tên cá nhân - Tên miền
Địa chỉ email (E)	Địa chỉ email của thuê bao sở hữu chứng thư chữ ký số
Định danh của thuê bao (UID)	MST:[mã số thuế] hoặc MNS:[mã quan hệ ngân sách] hoặc BHXX:[mã số bảo hiểm xã hội] hoặc hoặc HC:[số hộ chiếu] hoặc CCCD/CC:[số thẻ căn cước công dân/Căn cước] <i>Các trường hợp khác theo thỏa thuận giữa thuê bao và tổ chức cung cấp dịch vụ chứng thư chữ ký số.</i>

3.1.3 Ấn danh hoặc bút danh:

Thuê bao không được phép sử dụng tên ấn danh hoặc bút danh khác với tên thật của mình.

3.1.4 Quy tắc diễn giải các hình thức tên khác nhau:

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

3.1.5 Tính duy nhất của tên:

- Tên thuê bao sẽ là duy nhất gắn với một cặp chứng thư chữ ký số xác định trong dịch vụ HILO-CA.

- Một thuê bao có thể có hai hoặc nhiều chứng thư chữ ký số có cùng tên thuê bao.

3.1.6 Nhận diện, xác thực và vai trò của nhãn hiệu:

- Thuê bao đăng ký chứng thư chữ ký số không được sử dụng các tên đã được bảo hộ quyền sở hữu trí tuệ cho đối tượng khác theo quy định của pháp luật.
- Trong trường hợp cần thiết, HILO-CA sẽ yêu cầu đối tượng đăng ký chứng thư chữ ký số cung cấp các tài liệu chứng minh quyền sở hữu đối với tên đăng ký.
- Tuy nhiên, HILO-CA không chịu trách nhiệm về mọi tranh chấp về quyền sở hữu trí tuệ phát sinh liên quan đến việc sử dụng tên của đối tượng đăng ký chứng thư chữ ký số.
- Trường hợp cần thiết, HILO-CA có quyền chấm dứt hoặc tạm dừng bất cứ chứng thư chữ ký số nào liên quan đến các tranh chấp đã nêu.

3.2 Xác minh đề nghị phát hành chứng thư chữ ký số:

Quy trình tiếp nhận đề nghị phát hành chứng thư chữ ký số

Bước 1: Thuê bao đề nghị cấp chứng thư chữ ký số:

- Thuê bao (có thể là một cá nhân hoặc một đơn vị) đến trung tâm đăng ký chứng thư (HILO-RA), thực hiện yêu cầu cung cấp dịch vụ chữ ký số HILO-CA.
- Thuê bao điền thông tin vào đơn cấp chứng thư chữ ký số theo mẫu và cung cấp các giấy tờ liên quan.
- Thuê bao có 02 lựa chọn:
 - o Thuê bao tự sinh khóa: Điền đơn cấp chứng thư chữ ký số theo mẫu do HILO-CA cung cấp.
 - o Thuê bao yêu cầu CA sinh khóa: Điền đơn cấp chứng thư chữ ký số theo mẫu do HILO-CA cung cấp có tích vào phần yêu cầu HILO-CA sinh khóa cho thuê bao.
- HILO-CA tiếp nhận thông tin thuê bao đăng ký và chuyển hồ sơ sang giai đoạn xác minh.

Bước 2. Xác minh thông tin đề nghị phát hành chứng thư chữ ký số:

RA/CA thực hiện đối chiếu và xác nhận thông tin thuê bao bằng cách ký xác nhận đối chiếu bản sao với bản gốc, dưới hình thức ký điện tử hoặc ký tay, theo các điều kiện sau:

a) Điều kiện về nhân sự thực hiện:

- Là giao dịch viên, đại lý, cộng tác viên hoặc nhân viên kinh doanh được HILO-CA ủy quyền hợp lệ, có hồ sơ đăng ký và tài khoản được phê duyệt.
- Có thiết bị, phần mềm và môi trường làm việc đáp ứng yêu cầu kỹ thuật theo quy định pháp luật.

b) Điều kiện về chữ ký số và phần mềm ký:

- Phần mềm ký số phải đáp ứng yêu cầu kỹ thuật tại Thông tư số 22/2020/TT-BTTTT của Bộ Thông tin và Truyền thông(Nay là Bộ Khoa Học và Công nghệ) về phần mềm ký số và phần mềm kiểm tra chữ ký số.
- Chứng thư số sử dụng trong quá trình xác nhận:
 - o Cộng tác viên: sử dụng chữ ký số cá nhân;
 - o Đại lý (tổ chức): sử dụng chữ ký số doanh nghiệp;
 - o Nhân sự được đại lý ủy quyền: sử dụng chữ ký số cá nhân thuộc doanh nghiệp hoặc ký đồng thời bằng chữ ký số cá nhân và doanh nghiệp.

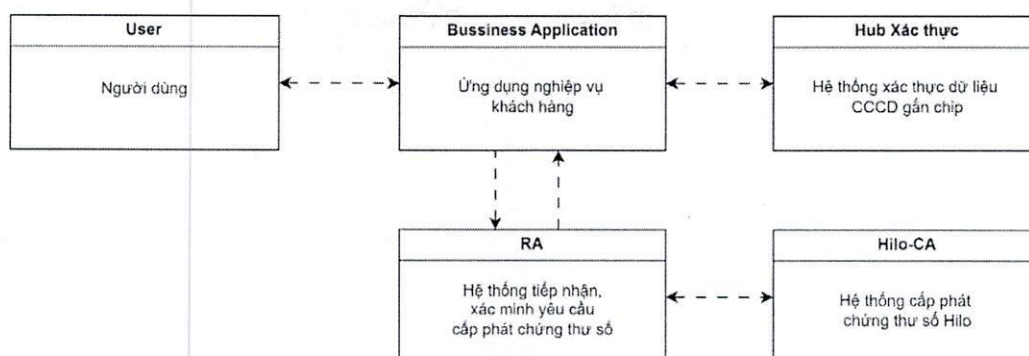
c) Phương thức xác minh thông tin thuê bao bao gồm 2 phương thức. Cụ thể:

1. Phương thức xác minh bằng phương pháp đối chiếu giấy tờ và tra cứu cơ sở dữ liệu

- HILO-CA tiến hành kiểm tra và xác minh tính chính xác của thông tin mà thuê bao cung cấp trong đơn đăng ký.
- Việc xác minh được thực hiện thông qua:
 - o Đối chiếu hồ sơ giấy tờ gốc mà thuê bao xuất trình;
 - o Tra cứu cơ sở dữ liệu điện tử của các cơ quan nhà nước, ví dụ:
 - +) Công thông tin người nộp thuế tại <https://tracuunnt.gdt.gov.vn> của Tổng cục Thuế;
 - +) Các nguồn dữ liệu định danh hợp lệ khác theo quy định.

2. Phương thức xác minh bằng phương pháp xác thực điện tử:

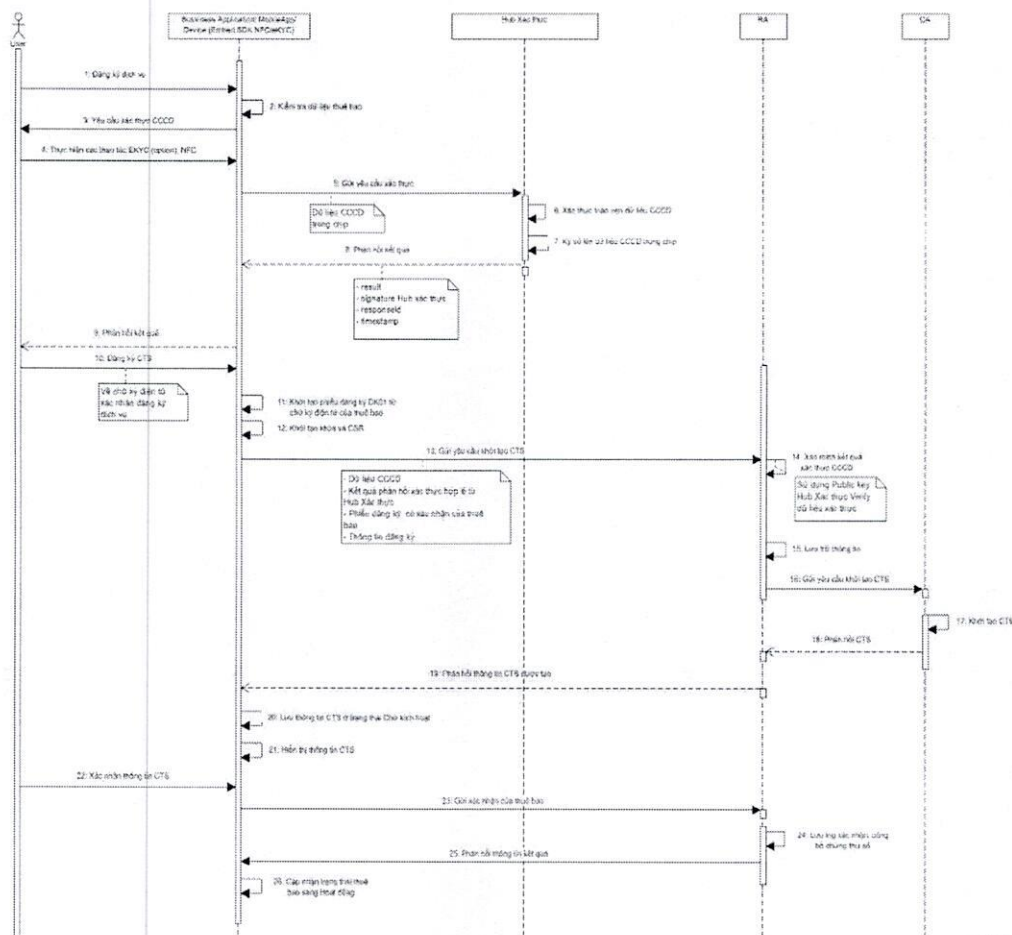
- **Mô hình kiến trúc**



- Mô tả thành phần

STT	Thành phần	Mô tả
1	User	Người dùng sử dụng thiết bị di động/ thiết bị đầu đọc có tích hợp SDK đọc NFC và xác thực khuôn mặt. Đăng ký dịch vụ và thực hiện xác thực CCCD.
2	Bussiness Application	- Hệ thống ứng dụng nghiệp vụ BackEnd thu thập dữ liệu từ CCCD gắn chip bằng NFC. Thực hiện kiểm tra sống (liveness) và so khớp khuôn mặt. - Sinh biểu mẫu đăng ký dịch vụ CTS. Tổng hợp hồ sơ và gửi đến CA. - Quản lý luồng xác thực và trạng thái CTS. Sinh CSR (Certificate Signing Request) vào thiết bị bảo mật HSM. - Thành phần này kết nối với CA (RA) thông qua APIKey và xác thực chéo (SSL/TLS 2 way) bằng certificate SSL được cấp phát từ HiloCA
3	Hub Xác thực	Đảm nhiệm vai trò dữ liệu toàn vẹn trong chip và ký xác thực dữ liệu được kiểm tra
4	RA	Xác minh hồ sơ từ Hub Ký số. Kiểm tra tính hợp lệ của giấy tờ và chữ ký số từ Hub Xác thực. Chuyển yêu cầu hợp lệ sang CA.
5	CA	Xử lý yêu cầu cấp chứng thư số (CTS). Phát hành chứng thư số và gửi lại RA

- **Luồng nghiệp vụ:**



Chi tiết luồng Quy trình nghiệp vụ:

Bước 1: Thu thập và xác thực danh tính điện tử (Điều 36 khoản 1 điểm a, b và Điều 36 khoản 2 điểm a, b Nghị định 23/2025/NĐ-CP):

- Người dùng sử dụng thiết bị di động hoặc đầu đọc có hỗ trợ NFC và camera để tương tác với CCCD gắn chip.
- Người dùng phải xác nhận đồng ý thu thập dữ liệu sinh trắc
- Ứng dụng nghiệp vụ thực hiện:
 - Đọc dữ liệu từ chip CCCD (QR Code, ảnh, dữ liệu sinh trắc học).
 - Thực hiện kiểm tra thực thể sống (liveness) và so khớp khuôn mặt
 - Gửi dữ liệu xác thực đến Hub Xác thực.
- Hub Xác thực:
 - Đảm bảo dữ liệu từ CCCD không bị sửa đổi.
 - Ký số lên dữ liệu xác thực và trả về kết quả gồm chữ ký số và timestamp.

Đảm bảo danh tính người dùng là hợp lệ, dữ liệu không bị can thiệp và có dấu vết thời gian tin cậy

Bước 2: Khởi tạo hồ sơ đề nghị cấp CTS (Điều 36 khoản 1 điểm c và Điều 38 khoản 3 Nghị định 23/2025/NĐ-CP)

- Sau khi xác thực thành công:
 - Hệ thống nghiệp vụ sinh biểu mẫu đề nghị đăng ký chứng thư số (DK-01).
 - Khởi tạo cặp khóa (private/public) trong thiết bị bảo mật HSM hoặc thiết bị đầu cuối.
 - Sinh CSR (Certificate Signing Request) chứa public key và thông tin người dùng.
 - Biểu mẫu và dữ liệu được ký điện tử bởi người dùng hoặc đại diện hệ thống.

Các dữ liệu đầu ra: DK-01 (PDF/XML), CSR, metadata định danh, log chứng thực đảm bảo tính xác thực

Bước 3: Gửi hồ sơ tới RA/CA (Điều 36 khoản 2 điểm b và Điều 38 khoản 4 Nghị định 23/2025/NĐ-CP):

- Hồ sơ được gửi đến RA (Registration Authority) bao gồm:
 - CCCD số hóa (nội dung trích xuất từ chip).
 - Kết quả xác thực từ Hub (gồm chữ ký số, timestamp).
 - Biểu mẫu DK-01 đã ký số.
 - File CSR.
- RA:
 - Kiểm tra tính hợp lệ của hồ sơ.
 - Xác minh chữ ký số từ Hub bằng Public Key gốc đã được CA công nhận.
 - Nếu hợp lệ, RA chuyển hồ sơ sang CA.

Ghi log toàn bộ quá trình xác minh, trạng thái hồ sơ, mã hồ sơ yêu cầu cấp phát

Bước 4: Cấp phát chứng thư số (Điều 38 khoản 2 & 3 Nghị định 23/2025/NĐ-CP)

- CA tiếp nhận hồ sơ:

- Kiểm tra nội dung CSR và xác thực lại các thông tin định danh.
- Phát hành chứng thư số (CTS) cho người dùng theo chuẩn X.509.
- Gửi chứng thư số trở lại RA → Ứng dụng nghiệp vụ → thiết bị người dùng.

Đảm bảo kết nối bảo mật 2 chiều (SSL/TLS mutual authentication) trong giao tiếp giữa CA và hệ thống.

Bước 5: Xác nhận và công bố chứng thư (Điều 38 khoản 4 Nghị định 23/2025/NĐ-CP)

- Người dùng nhận CTS:
 - Hệ thống yêu cầu người dùng ký xác nhận đã nhận CTS.
 - Kết quả xác nhận được lưu lại dưới dạng bản ghi (log + DB).
- Ứng dụng cập nhật:
 - Trạng thái chứng thư (đã cấp, đã xác nhận).
 - Gửi bản sao kết quả xác nhận lên CA.
- CA:
 - Cập nhật trạng thái chứng thư số.
 - Công bố CTS trên hệ thống tra cứu CTS công cộng (OCSP/CRL hoặc LDAP tùy cấu hình).

Bước 6: Ghi log và lưu trữ (Điều 36 khoản 2 điểm g và Điều 37 khoản 5 Nghị định 23/2025/NĐ-CP):

- Mọi thao tác hệ thống (gồm truy xuất CCCD, xác thực, tạo hồ sơ, cấp phát, xác nhận) đều được:
 - Ghi log đầy đủ theo định dạng chuẩn (JSON hoặc XML).
 - Lưu trữ trên hệ thống MinIO, phục vụ kiểm tra sau này.
 - Có phân quyền truy cập, mã hóa dữ liệu nhạy cảm.

Xử lý lỗi & dự phòng (Điều 36 khoản 2 điểm d, e, g và Điều 37 khoản 5 điểm a,b,c Nghị định 23/2025/NĐ-CP):

- ✓ Nếu xác thực thất bại → ghi lại lý do (mismatch sinh trắc học, chip lỗi...).
- ✓ Nếu hồ sơ không hợp lệ → thông báo rõ lý do từ RA.

- Log khách hàng xác nhận thông tin chứng thư số

```
2025-05-05 14:44:05,999 INFO vn.signid.ra.service.ca.impl.CertificateServiceImpl [http-nio-0720-exec-8] -----> Confirm certificate info, subject: C=VN, ST=Nghệ An, L=Núi L, Nam Thành, Nam Bàn, N  
ghệ An, CN=Nguyễn Tuấn Anh, UID=CCOD:849282825349
```

➔ Dữ liệu xác nhận được lưu trữ dưới DB

- Quy trình xác minh chi tiết cho từng loại thuê bao được quy định tại mục 3.2.2 và 3.2.3 của Quy chế này.

d) Xử lý kết quả xác minh:

- Trường hợp thông tin thuê bao không hợp lệ: HILO-CA từ chối tiếp nhận hồ sơ, thông báo lý do cụ thể và hướng dẫn thuê bao thực hiện lại thủ tục đăng ký.
- Trường hợp thông tin thuê bao hợp lệ: HILO-CA chuyển sang bước tạo khóa cho thuê bao và thực hiện quy trình phát hành chứng thư số.

3.2.1 Phương thức chứng minh quyền sở hữu khóa bí mật:

Thuê bao đăng ký chứng thư chữ ký số trong trường hợp thuê bao tự sinh khóa cần phải chứng minh đang sở hữu khóa bí mật hợp lệ.

Phương pháp chứng minh sở hữu khóa bí mật sẽ tuân theo chuẩn PKCS#10 chứa thông tin định danh của thuê bao và được ký sử dụng khóa bí mật của thuê bao.

Thuê bao cần cung cấp các thông tin liên quan cấu hình thiết bị phần cứng, phần mềm, thông tin thuê bao tương ứng với file request (.csr) cung cấp cho HILO-CA.

3.2.2 Xác minh danh tính đối với tổ chức:

HILO-CA thực hiện xác thực định danh của tổ chức thông qua bộ hồ sơ cấp chứng thư chữ ký số gồm:

- Phiếu đề nghị cấp chứng thư chữ ký số:
 - Phiếu đăng ký đúng mẫu do HILO-CA ban hành.
 - Thông tin doanh nghiệp điền trong phiếu chính xác.
 - Người đại diện pháp luật của tổ chức ký và đóng dấu tổ chức.
 - Trường hợp người ủy quyền ký thay cần kiểm tra thêm giấy ủy quyền có hợp lệ không.
- Giấy tờ kèm theo để xác thực gồm:

- 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 hoặc giấy chứng nhận đăng ký hộ kinh doanh;
 - Giấy tờ tùy thân của người đại diện theo pháp luật của tổ chức, bao gồm thẻ căn cước công dân hoặc thẻ căn cước hoặc giấy chứng nhận căn cước hoặc tài khoản định danh điện tử mức độ 2(VNEID) hoặc hộ chiếu; hoặc tài khoản định danh điện tử của tổ chức;
 - Các giấy tờ khác (nếu có): Giấy ủy quyền, giấy bổ nhiệm, giấy phân công công việc....
- 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.

Sau quá trình xác thực định danh cho tổ chức, bộ phận nghiệp vụ HILO-CA phải trả kết quả xác thực hồ sơ là hợp lệ hay không hợp lệ (ghi rõ lý do).

3.2.3 Xác minh danh tính đối với cá nhân:

HILO-CA thực hiện xác thực định danh của cá nhân thông qua bộ hồ sơ cấp chứng thư chữ ký số. Các thông tin cần xác thực gồm:

- Phiếu đề nghị cấp chứng thư chữ ký số:
 - Phiếu có nguyên vẹn mẫu của HILO-CA cung cấp.
 - Thuê bao điền đã đầy đủ thông tin trong phiếu.
 - Chủ thuê bao đã ký xác nhận vào mẫu.
- Giấy tờ kèm theo để xác thực gồm:
 - Giấy tờ tùy thân bao gồm thẻ căn cước công dân hoặc thẻ căn cước hoặc căn cước điện tử hoặc giấy chứng nhận căn cước hoặc tài khoản định danh điện tử mức độ 2(VNEID) hoặc hộ chiếu còn thời hạn; thị thực nhập cảnh còn thời hạn hoặc giấy tờ chứng minh được miễn thị thực nhập cảnh (đối với cá nhân là người nước ngoài);
 - Giấy ủy quyền (nếu có) và các giấy tờ khác.
- Thuê bao có quyền lựa chọn nộp bản sao từ giấy tờ gốc, bản sao có chứng thực hoặc nộp bản sao xuất trình kèm bản chính để đối chiếu.

- Một số thông tin khác cá nhân có thể bổ sung để việc xác thực được tốt hơn gồm: Địa chỉ thư điện tử; Thông tin về website, quyền sở hữu tên miền của cá nhân (dùng cho việc cấp chứng thư chữ ký số SSL).

Xác thực định danh cá nhân thuộc tổ chức:

Việc xác thực định danh để cấp cá nhân thuộc tổ chức thực hiện như việc xác thực định danh tổ chức và thêm các thủ tục sau:

- Xác thực thông tin cá nhân (theo giấy tờ tùy thân và thông tin tin cậy được công bố).
- Xác thực vị trí công tác (Phòng ban, chức vụ, quyền hạn) của cá nhân trong tổ chức.

Sau quá trình xác thực định danh cho tổ chức, bộ phận nghiệp vụ HILO-CA phải trả kết quả xác thực hồ sơ là hợp lệ hay không hợp lệ (ghi rõ lý do).

3.2.4 Thông tin thuê bao không được xác minh:

Các thông tin thuê bao không xác minh bao gồm:

- Thông tin phòng ban trong tổ chức của thuê bao.
- Các thông tin không cần xác thực trong chứng thư.

3.2.5 Xác minh thẩm quyền:

- Các tài liệu do tổ chức cung cấp (quyết định bổ nhiệm, phân công công việc...).
- Văn bản xác nhận có chữ ký số đang hoạt động hoặc con dấu của tổ chức.
- Đối chiếu với cơ sở dữ liệu nội bộ của tổ chức (nếu có liên thông).

3.2.6 Tiêu chí liên thông:

HILO-CA tuân thủ theo các quy định về liên thông giữa các hệ thống chứng thực chữ ký số do Bộ Khoa học và Công nghệ ban hành.

3.3 Xác minh đề nghị thay đổi khóa:

Quy trình tiếp nhận đề nghị thay đổi khóa:

Để thực hiện thủ tục thay đổi khóa, Thuê bao cần đến gặp HILO-RA và thực hiện các bước sau:

- Điền thông tin vào phiếu đề nghị thay đổi khóa và nộp lại cho HILO-RA.

- HILO-RA tiến hành tiếp nhận và xác minh đề nghị thay đổi khóa.
- Thuê bao chờ HILO-RA xác minh đề nghị thay đổi khóa.

Đối với trường hợp thuê bao không đến trực tiếp có thể gửi hồ sơ đầy đủ theo đường bưu điện đến cho HILO-RA.

3.3.1 Xác minh danh tính và xác thực đối với yêu cầu thay đổi cặp khóa định kỳ:

Thủ tục xác minh đề nghị thay đổi cặp khóa của thuê bao:

- Sau khi HILO-RA tiếp nhận phiếu đề nghị thay đổi cặp khóa của thuê bao. HILO-RA cần xác minh để đảm bảo rằng cá nhân/tổ chức đề nghị thay đổi cặp khóa là chủ thuê bao của chứng thư chữ ký số đó.
- Thuê bao cần cung cấp thêm thông tin để xác minh đủ thẩm quyền yêu cầu thay đổi cặp khóa:
 - o Thuê bao cung cấp hợp đồng đã ký với HILO-CA (hoặc hóa đơn VAT do HILO-CA xuất), giấy đăng ký kinh doanh để chứng minh thuê bao là hợp lệ.
 - o Ngoài ra, thuê bao cần cung cấp thêm giấy tờ tùy thân (CC/CCCD/HC), giấy ủy quyền (trong trường hợp được ủy quyền).
- Phần HILO-RA xác minh các thông tin trên phiếu đề nghị thay đổi cặp khóa tương tự phần 3.2 Xác minh đề nghị cấp chứng thư chữ ký số.
- HILO-RA tra cứu hệ thống theo thông tin thuê bao cung cấp để tìm thông tin thuê bao.
 - o Nếu tồn tại chứng thư chữ ký số của thuê bao hợp lệ: Trả kết quả xác minh thông tin thành công, chuyển bước tiếp theo.
 - o Nếu không tồn tại chứng thư chữ ký số của thuê bao hoặc thông tin thuê bao không hợp lệ hoặc hợp đồng với thuê bao đã hết hiệu lực (chứng thư chữ ký số hết hạn) thì trả kết quả xác minh không thành công, ghi rõ lý do và hướng dẫn thuê bao các thủ tục khác.

Thuê bao không được phép thay cặp khóa nếu thuộc một trong các trường hợp sau:

- HILO-CA phát hiện ít nhất 1 thông tin cần xác minh trong chứng thư chữ ký số không đúng.

- Chứng thư chữ ký số được sử dụng trong các hoạt động phạm pháp, các hoạt động có thể ảnh hưởng tới uy tín của HILO-CA.

3.3.2 Xác minh danh tính và xác thực đối với yêu cầu thay đổi cặp khóa sau khi thu hồi:

Nghị định 23 có các quy định về thu hồi chứng thư chữ ký số công cộng (Điều 42) và tạm dừng (Điều 41)

- Nếu chứng thư chữ ký số đã bị thu hồi thì thuê bao không được phép thay đổi cặp khóa, vì theo quy định khi chứng thư bị thu hồi thì quan hệ chứng thư chữ ký số đó chấm dứt và không có hiệu lực
- Ngoài ra, nếu phát hiện sai lệch thông tin trong chứng thư, hoặc chứng thư bị sử dụng cho mục đích trái phép, ảnh hưởng tới uy tín của tổ chức cung cấp dịch vụ chứng thực – cũng là các căn cứ để thu hồi hoặc từ chối yêu cầu.

3.4 Xác thực định danh cho yêu cầu thu hồi chứng thư số

3.4.1 Quy trình đề nghị thu hồi chứng thư chữ ký số.

Chứng thư chữ ký số sẽ bị thu hồi (Điều 42) trong các trường hợp sau:

- o Khi thuê bao yêu cầu bằng văn bản và xác minh đề nghị thu hồi là chính xác.
- o Theo yêu cầu từ các cơ quan nhà nước có Thẩm Quyền.
- o Thuê bao là cá nhân đã chết hoặc mất tích theo tuyên bố của tòa án, hoặc tổ chức đã giải thể/phá sản theo quy định pháp luật.
- o HILO-CA phát hiện các sự cố an ninh, truy cập hoặc sử dụng trái phép, cần thu hồi hoặc tạm dừng chứng thư chữ ký số.

Để thực hiện thu hồi chứng thư chữ ký số, thuê bao cần thực hiện các bước như sau:

1. Thuê bao gửi đề nghị thu hồi chứng thư chữ ký số đến HILO-CA.
2. HILO-RA tiến hành xác minh đề nghị thu hồi chứng thư chữ ký số.
3. Thuê bao đợi HILO-RA trả kết quả và hướng dẫn thủ tục tiếp theo.

3.4.2 Thủ tục xác minh đề nghị thu hồi chứng thư chữ ký số:

Xác minh tính hợp lệ của hồ sơ:

1. Hồ sơ đúng thẩm quyền của các cơ quan.
2. Hồ sơ của thuê bao đề nghị đúng mẫu do HILO-CA cung cấp.

3. Chủ thuê bao đã điền đủ thông tin, ký và xác nhận vào phiếu đề nghị thu hồi chứng thư chữ ký số

4. Người thực hiện đề nghị thu hồi chứng thư chữ ký số là chủ hợp pháp của thuê bao (hoặc người ủy quyền hợp pháp).

- Người thực hiện cung cấp hợp đồng (hoặc hóa đơn VAT do HILO-CA xuất), đăng ký kinh doanh của doanh nghiệp(Nếu là tổ chức);
- Người thực hiện cung cấp giấy tờ tùy thân(CC/CCCD/HC) phải còn hiệu lực, phần xác minh sinh trắc học nếu yêu cầu, và các biện pháp kỹ thuật (nếu có sự khác biệt dấu hiệu bất thường) thì phải từ chối hoặc xác minh thêm.
- Giấy ủy quyền (nếu thực hiện theo ủy quyền).

⇒ Nếu xác minh hồ sơ đề nghị thu hồi chứng thư chữ ký số hợp lệ thì HILO-RA thực hiện chuyển bước tiếp theo. Nếu không hợp lệ thì trả đề nghị lại thuê bao, ghi rõ lý do từ chối.

Xác minh thông tin thuê bao trong hệ thống: HILO-CA thực hiện tìm kiếm chứng thư chữ ký số của thuê bao trong hệ thống.

1. Tìm thấy chứng thư chữ ký số của thuê bao hợp lệ: Trả kết quả xác minh cho kết quả thành công. Chuyển bước tiếp theo.

2. Nếu không thấy chứng thư chữ ký số hoặc thông tin người thực hiện cung cấp bị sai hoặc chứng thư chữ ký số hết hạn: Trả kết quả xác minh không thành công, ghi rõ lý do và hướng dẫn thực hiện bước tiếp theo.

4. CÁC YÊU CẦU ĐỐI VỚI VÒNG ĐỜI HOẠT ĐỘNG CỦA CHỨNG THƯ CHỮ KÝ SỐ:

4.1 Yêu cầu đề nghị phát hành chứng thư chữ ký số:

4.1.1 Đối tượng đề nghị phát hành chứng thư chữ ký số:

Đối tượng đề nghị phát hành chứng thư chữ ký số gồm:

- Tổ chức, cá nhân cư trú, sinh sống, làm việc tại Việt Nam, có nhu cầu sử dụng chứng thư chữ ký số, và đáp ứng đầy đủ các điều kiện theo quy định của pháp luật hiện hành và Chính sách chứng thực (CPS) do HILO-CA ban hành.

Người đại diện theo pháp luật của tổ chức:

- Là người đứng tên đại diện pháp nhân hoặc tổ chức theo đăng ký pháp lý;

- Đủ điều kiện thực hiện giao dịch ký số thay mặt tổ chức theo quy định tại Điều lệ hoạt động hoặc theo giấy tờ pháp lý của tổ chức;
- Có nhu cầu đăng ký sử dụng chứng thư chữ ký số để phục vụ hoạt động nghiệp vụ, hành chính hoặc giao dịch điện tử.

Người được ủy quyền thực hiện đăng ký hoặc sử dụng chứng thư chữ ký số (nếu có), trong đó:

- Việc ủy quyền phải được thể hiện bằng văn bản hợp lệ, có chữ ký hoặc chữ ký số của người đại diện theo pháp luật và dấu (nếu có);
- Người được ủy quyền phải cung cấp giấy tờ tùy thân hợp lệ (CC/CCCD/Hộ chiếu) và giấy ủy quyền còn hiệu lực.

4.1.2 Trách nhiệm và quy trình đăng ký:

a) Trách nhiệm của các bên liên quan:

Thuê bao (cá nhân hoặc tổ chức đề nghị cấp chứng thư chữ ký số)

- Cung cấp thông tin chính xác, đầy đủ theo mẫu đăng ký được quy định.
- Xuất trình và/hoặc nộp giấy tờ chứng minh danh tính hợp lệ:
 - Đối với cá nhân: CC/CCCD/Hộ chiếu còn hiệu lực.
 - Đối với tổ chức: 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 hoặc giấy chứng nhận đăng ký hộ kinh doanh và giấy tờ tùy thân của người đại diện theo pháp luật của tổ chức, bao gồm thẻ căn cước công dân hoặc thẻ căn cước hoặc giấy chứng nhận căn cước hoặc tài khoản định danh điện tử mức độ 2(VNEID) hoặc hộ chiếu; hoặc tài khoản định danh điện tử của tổ chức. Giấy ủy quyền (nếu có).
- Chịu trách nhiệm về tính chính xác, trung thực của các thông tin đã khai báo.
- Tuân thủ quy định sử dụng chứng thư chữ ký số, bảo mật khóa riêng.
- Thanh toán đầy đủ các phí, lệ phí liên quan (nếu có).

Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng (HILO-CA):

- Tiếp nhận, kiểm tra, xác minh tính hợp lệ của hồ sơ đăng ký.
- Thực hiện định danh và xác thực thuê bao theo quy định tại Nghị định 23/2025/NĐ-CP và Chính sách chứng thực (CPS).

- Phát hành chứng thư chữ ký số sau khi hồ sơ hợp lệ và thủ tục xác minh hoàn tất.
- Lưu trữ hồ sơ, dữ liệu phát hành chứng thư đúng thời hạn pháp luật quy định.

Cập nhật thông tin chứng thư lên hệ thống tra cứu trực tuyến.

Đại lý đăng ký (Registration Authority – RA) hoặc Bộ phận hỗ trợ của Kinh doanh (nếu có):

- Tiếp nhận hồ sơ ban đầu và hướng dẫn khách hàng.
- Kiểm tra sơ bộ hồ sơ và chuyển về HILO-CA để xử lý.
- Hỗ trợ người dùng hoàn thiện thủ tục định danh và kích hoạt chứng thư.

b) Quy trình đăng ký phát hành chứng thư chữ ký số:

Bước 1: Chuẩn bị hồ sơ đăng ký:

Hồ sơ bao gồm:

- Phiếu đăng ký phát hành chứng thư chữ ký số (theo mẫu của HILO-CA).
- Bản sao giấy tờ tùy thân (CC/CCCD/Hộ chiếu đối với cá nhân).
- Giấy phép đăng ký kinh doanh, quyết định bổ nhiệm (nếu là tổ chức).
- Giấy ủy quyền (nếu người thực hiện không phải là người đại diện pháp luật).
- Thông tin kỹ thuật cần thiết (địa chỉ email, thiết bị lưu khóa, HSM, token...).

Bước 2: Nộp hồ sơ và thực hiện định danh:

- Hồ sơ được nộp trực tiếp tại điểm giao dịch RA hoặc qua hệ thống trực tuyến.
- Nhân viên RA/CA thực hiện kiểm tra giấy tờ gốc, đối chiếu thông tin mục 3.2
- Định danh và xác thực cá nhân theo một trong các phương thức:
 - Gặp mặt trực tiếp (face-to-face).
 - Qua video call có xác minh (nếu được CA hỗ trợ).
 - Qua tài khoản định danh điện tử (mức 2 trở lên) hoặc Căn cước công dân/Căn cước gắn chip (nếu tích hợp hệ thống).

Bước 3: Xử lý và cấp chứng thư chữ ký số:

- Sau khi xác minh hồ sơ hợp lệ, CA thực hiện:

- Tạo cặp khóa công khai – bí mật (nếu người dùng không tự tạo).
- Cấp chứng thư chữ ký số, gắn với khóa công khai và thông tin đã xác thực.
- Cập nhật thông tin chứng thư vào CSDL chứng thư và CRL/OCSP.

Bước 4: Bàn giao và hướng dẫn sử dụng:

- Gửi chứng thư chữ ký số qua email hoặc bàn giao thiết bị chứa khóa (USB token, SIM ký số, thiết bị HSM...).
- Hướng dẫn cài đặt, sử dụng phần mềm ký số.
- Yêu cầu người dùng kiểm tra và xác nhận lại thông tin chứng thư.

Bước 5: Lưu trữ hồ sơ và hậu kiểm:

- HILO-CA lưu trữ toàn bộ hồ sơ, nhật ký xử lý theo thời hạn quy định tại Điều 50 Nghị định 23/2025.
- Có thể tiến hành hậu kiểm hoặc cập nhật lại thông tin định kỳ theo yêu cầu.

⇒ **Lưu ý quan trọng:**

- Không phát hành chứng thư trong các trường hợp:
 - Hồ sơ không hợp lệ, thiếu giấy tờ.
 - Phát hiện thông tin sai lệch, giả mạo.
 - Người dùng thuộc danh sách bị từ chối cấp (theo luật hoặc yêu cầu cơ quan chức năng).
- Việc phát hành chứng thư chữ ký số phải được hoàn thành trong thời hạn không quá 05 ngày làm việc kể từ khi nhận đủ hồ sơ hợp lệ.

4.2 Xử lý yêu cầu đề nghị phát hành chứng thư chữ ký số:

4.2.1 Thực hiện chức năng xác minh danh tính và xác thực:

HILO-CA tiến hành xác thực định danh tất cả các thông tin của thuê bao yêu cầu cấp chứng thư chữ ký số theo phần 3.2

4.2.2 Phê duyệt hoặc từ chối hồ sơ đề nghị phát hành chứng thư chữ ký số:

HILO-CA chỉ chấp nhận yêu cầu cấp chứng thư chữ ký số nếu thỏa mãn tất cả các điều kiện xác minh thông tin, ký hợp đồng và nộp đầy đủ phí dịch vụ cấp chứng thư chữ ký số cho HILO-CA.

HILO-CA từ chối yêu cầu cấp chứng thư chữ ký số trong các trường hợp sau:

- Xác thực định danh không thành công ít nhất một trong các thông tin về đối tượng yêu cầu cấp chứng thư chữ ký số theo mục 3.2;
- Đối tượng yêu cầu cấp chứng thư chữ ký số không cung cấp đủ tài liệu theo yêu cầu;
- Đối tượng yêu cầu cấp chứng thư chữ ký số không trả lời yêu cầu liên lạc trong hạn thời gian xác định;
- Đối tượng yêu cầu cấp chứng thư chữ ký số chưa thanh toán phí dịch vụ cấp chứng thư chữ ký số;
- Có căn cứ cho rằng việc HILO-CA cấp chứng thư chữ ký số cho đối tượng yêu cầu có thể ảnh hưởng tới uy tín và độ tin cậy của HILO-CA.

4.2.3 Thời gian xử lý hồ sơ đề nghị phát hành chứng thư chữ ký số:

HILO-CA có trách nhiệm xử lý yêu cầu cấp chứng thư chữ ký số trong một khoảng thời gian phù hợp. Không quy định thời gian hoàn thành quá trình xử lý một yêu cầu cấp chứng thư chữ ký số trừ khi có thỏa thuận trong Hợp đồng dịch vụ hoặc CPS, tuy nhiên thời gian tối đa là 5 ngày làm việc. Yêu cầu cấp chứng thư chữ ký số sẽ ở trạng thái có hiệu lực cho tới khi bị HILO-CA từ chối.

4.3 Phát hành chứng thư chữ ký số:

4.3.1 Quy trình phát hành chứng thư chữ ký số:

Để phát hành chứng thư chữ ký số, thuê bao đều phải ký Hợp đồng dịch vụ với HILO-CA sau khi thực hiện quy trình đăng ký bao gồm:

Bước 1: Đăng ký cấp chứng thư chữ ký số:

- Thuê bao (có thể là một cá nhân hoặc một đơn vị) đến văn phòng giao dịch/ủy quyền của HILO-CA hoặc tải danh mục hồ sơ cấp chứng thư chữ ký số trên website <https://HILO-CA.vn/tai-lieu/>
- Thuê bao điền thông tin vào đơn cấp chứng thư chữ ký số theo mẫu và cung cấp các giấy tờ liên quan gửi cho HILO-CA theo quy định tại 4.1.2
- Trong phiếu đăng ký cấp chứng thư chữ ký số thuê bao có 02 lựa chọn:
 - o Thuê bao tự sinh khóa: Điền đơn cấp chứng thư chữ ký số theo mẫu do HILO-CA cung cấp.

- Thuê bao yêu cầu CA sinh khóa: Điền đơn cấp chứng thư chữ ký số theo mẫu do HILO-CA cung cấp có tích vào phần yêu cầu HILO-CA sinh khóa cho thuê bao.
- HILO-CA tiếp nhận thông tin thuê bao đăng ký, thuê bao đợi kết quả xác minh yêu cầu cấp chứng thư chữ ký số.

Bước 2: HILO-CA xác minh thông tin thuê bao trên phiếu đề nghị cấp chứng thư chữ ký số

- HILO-CA thực hiện việc xác minh thông tin thuê bao theo quy định tại phần 3.
- Nếu thông tin thuê bao không hợp lệ, HILO-CA thông báo từ chối cấp chứng thư chữ ký số (ghi rõ lý do).
- Nếu thông tin thuê bao hợp lệ:
 - HILO-CA bàn giao thiết bị Usb Token đạt chuẩn cho thuê bao và hướng dẫn thuê bao cách tạo khóa hoặc tải liệu yêu cầu đối bảo mật với thiết bị HSM nếu thuê bao chọn tự sinh khóa.
 - HILO-CA nhập thông tin thuê bao, đính kèm cái tài liệu lên hệ thống quản lý khách hàng.
 - HILO-CA gửi yêu cầu cấp chứng thư chữ ký số tới hệ thống, chuyển sang bước tạo khóa cho thuê bao.

Bước 3: Tạo khoá và chứng thư chữ ký số:

Để tạo khóa và chứng thư chữ ký số thì HILO-CA có 02 cách tương ứng với lựa chọn là thuê bao tự tạo khóa và thuê bao yêu cầu sinh khóa hộ như sau:

- Trường hợp thuê bao tự tạo khóa:
 - Thuê bao tạo khóa từ thiết bị Usb Token/HSM theo hướng dẫn.
 - Thuê bao gửi yêu cầu cấp chứng thư chữ ký số về cho HILO-CA (định dạng file .csr) theo chuẩn PKCS#10.
 - HILO-CA tiếp nhận CSR của thuê bao.
 - HILO-CA kiểm tra thông tin trên yêu cầu cấp CTS. Các thông tin cần xác minh gồm:
 - Các trường quy định tên như quy định tại phần 1.
 - Xác minh thông tin trong file .csr với thông tin thuê bao đã được xác minh từ bộ phận thẩm định. Kiểm tra, so khớp thông tin trong hệ thống và thông tin trên hồ sơ đăng ký.
 - Cấu hình thiết bị phần cứng đáp ứng tiêu chuẩn mật mã.

- Hệ thống HILO-CA tạo dữ liệu chứng thư chữ ký số dưới dạng chuẩn X509 v3. Hệ thống HILO-CA gửi yêu cầu ký chứng thư chữ ký số tới HSM, HSM sẽ thực hiện ký chứng thư chữ ký số cho thuê bao tạo ra chứng số chuẩn X509.
- Hệ thống HILO-CA sẽ lưu trữ vào cơ sở dữ liệu của HILO-CA các thông tin của thuê bao: Hồ sơ thông tin thuê bao; Request yêu cầu cấp phát chứng thư PKCS#10; Chứng thư chữ ký số của thuê bao. Hệ thống cập nhật dữ liệu chứng thư chữ ký số vào LDAP. Hệ thống cập nhật trạng thái chứng thư chữ ký số vừa được cấp phát vào Database OCSP của HILO-CA
- Trường hợp thuê bao yêu cầu CA tạo khóa:
 - HILO-CA kiểm tra lại thông tin thuê bao trong hệ thống, gói cước yêu cầu.
 - HILO-CA tạo khóa và chứng thư chữ ký số cho thuê bao trong thiết bị USB Token đạt chuẩn (như trên).

4.3.2 Thông báo việc phát hành chứng thư chữ ký số:

Quy định ở phần tiếp theo.

Lưu ý:

- Đối với các tệp, vì trong đó có khoá bí mật đã được mã hoá (sử dụng mật khẩu khi tạo tệp này), do vậy khi gửi đến máy ghi cần gửi kèm danh sách mật khẩu tương ứng.
- Sau mỗi lần ghi xong một USB Token, trung tâm quản lý chứng thư thực hiện điền vào một danh sách thông tin về chứng thư được lưu trên USB Token đó và gửi về cho trung tâm đăng ký để chuyển đến thuê bao.

4.4 Xác nhận và công bố công khai chứng thư chữ ký số:

4.4.1 Xác nhận các thông tin trên chứng thư chữ ký số được cấp là chính xác:

Thuê bao sẽ xác nhận thông tin trên chứng thư chữ ký số được cấp là chính xác qua hai bước.

- Về mặt kỹ thuật, trong quá trình tạo chứng thư chữ ký số, hệ thống HILO-CA có màn hình hiển thị thông tin thuê bao để tạo chứng thư chữ ký số. Thuê bao kiểm tra thông tin thuê bao:
 - Nếu thông tin thuê bao đúng: Thuê bao chấp nhận và chuyển bước tiếp theo để tạo chứng thư chữ ký số.

- Nếu thông tin thuê bao không đúng: Thuê bao hủy quá trình tạo chứng thư chữ ký số và thực hiện lại.
- Đồng thời, các quá trình tạo khóa, tạo chứng thư chữ ký số, HILO-CA đều gửi email ghi đầy đủ thông tin, gói cước để thông báo cho thuê bao về việc cấp chứng thư chữ ký số. Thuê bao cần gửi email xác nhận thông tin là đúng đối với HILO-CA. Nếu thuê bao không phản hồi với HILO-CA trong khoảng thời gian 3 ngày, chứng thư chữ ký số coi như được thuê bao chấp nhận.

- Về mặt hồ sơ:

Sau khi nhận được chứng thư chữ ký số, thuê bao có trách nhiệm kiểm tra và xác nhận tính chính xác của thông tin ghi trên chứng thư. Việc xác nhận được thực hiện theo một trong hai hình thức sau:

- Xác nhận trực tiếp (Offline): Thuê bao điền thông tin vào Phiếu xác nhận thông tin chứng thư số, theo mẫu do HILO-CA ban hành. Người đại diện hợp lệ của thuê bao ký tên và đóng dấu (đối với tổ chức), sau đó gửi phiếu xác nhận về HILO-CA để lưu hồ sơ.

Link: <https://HILO-CA.vn/tai-lieu/>

- Xác nhận trực tuyến (Online): Thuê bao thực hiện xác nhận thông tin bằng chữ ký điện tử trên hệ thống. Hệ thống của HILO-CA sẽ ghi nhận log trên hệ thống bao gồm: địa chỉ IP, thời gian thuê bao xác nhận đã được ghi nhận đầy đủ. Và lưu trữ làm bằng chứng cho việc xác nhận.

Trường hợp thuê bao không thực hiện xác nhận trong thời hạn 01 (một) tháng kể từ ngày chứng thư được cấp, HILO-CA có quyền tạm dừng hiệu lực của chứng thư chữ ký số nhằm hạn chế rủi ro cho thuê bao và đảm bảo an toàn thông tin.

4.4.2 Công bố chứng thư chữ ký số theo quy định:

HILO-CA sẽ thực hiện công bố công khai và quản lý hệ thống danh bạ về chứng thư chữ ký số của thuê bao ngay sau khi hoàn thành thủ tục cấp chứng thư chữ ký số cho thuê bao tại website <https://HILO-CA.vn>. Hệ thống danh bạ chứng thư chữ ký số HILO-CA công bố bao gồm:

- Chứng thư chữ ký số của HILO-CA: truy cập chức năng theo đường dẫn <https://HILO-CA.vn/tai-lieu/>

- Chứng thư chữ ký số của thuê bao và kiểm tra trạng thái chứng thư chữ ký số: truy cập chức năng theo đường dẫn <https://HILO-CA.vn/tra-cuu-cts/>
- Danh sách Chứng thư chữ ký số thu hồi (CRL): truy cập chức năng theo đường dẫn <http://crl.HILO-CA.vn/hiloca.crl>
- Quy chế chứng thực chữ ký số HILO-CA và các thông tin khác: truy cập chức năng theo đường dẫn <https://HILO-CA.vn/tai-lieu/>

4.4.3 Thông báo đến các đối tượng khác về việc phát hành chứng thư chữ ký số:

HILO-CA công bố thông tin tới các thành phần liên quan hệ thống như sau:

- Email công bố thông tin chứng thư chữ ký số tới thuê bao theo email thuê bao đã đăng ký.
- Cung cấp thông tin tới ROOT-CA theo quy định.

HILO-CA thực hiện công bố tài liệu hướng dẫn thuê bao tra cứu thông tin chứng thư chữ ký số trực tuyến tại địa chỉ website: <https://HILO-CA.vn/tai-lieu/>

4.5 Sử dụng cặp khóa và chứng thư chữ ký số:

Sau khi thuê bao được tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp chứng thư chữ ký số thì có thể sử dụng cặp khóa cũng như chứng thư chữ ký số của mình một cách hợp pháp theo các quy định của pháp luật.

4.5.1 Cách sử dụng chứng thư chữ ký số và khóa bí mật của thuê bao:

Việc sử dụng khóa bí mật tương ứng với khóa công khai trong chứng thư chữ ký số chỉ được cho phép khi thuê bao chấp nhận chứng thư chữ ký số. Chứng thư chữ ký số sẽ được sử dụng hợp pháp dựa trên các điều khoản của Hợp đồng dịch vụ, các điều khoản trong CPS này cũng như quy định của pháp luật.

Cách sử dụng chứng thư chữ ký số phải tương ứng với giá trị quy định của trường KeyUsage bên trong chứng thư chữ ký số (Ví dụ nếu giá trị Digital Signature không có trong trường KeyUsage thì chứng thư chữ ký số này không thể được dùng để ký điện tử).

Thuê bao có trách nhiệm bảo vệ khóa bí mật khỏi việc sử dụng bất hợp pháp và sẽ không được sử dụng khóa bí mật khi chứng thư chữ ký số hết hạn hay bị thu hồi.

4.5.2 Cách sử dụng khóa công khai và chứng thư chữ ký số bởi các bên tin tưởng:

Người nhận sẽ được HILO-CA đảm bảo các điều khoản về độ tin cậy của chứng thư chữ ký số. Độ tin cậy của chứng thư chữ ký số được xác định dựa vào từng hoàn cảnh cụ thể. Nếu hoàn cảnh chỉ ra rằng cần phải thêm sự bảo đảm, thì người nhận phải đạt được sự bảo đảm mà nó cần phải có. Trước khi được tin cậy, người nhận sẽ được đánh giá một cách độc lập các yếu tố sau:

- Chứng thư chữ ký số được sử dụng vào các mục đích phù hợp và xác định rằng các mục đích đó không bị cấm hoặc bị giới hạn bởi HILO-CA, CPS hay các quy định của pháp luật. HILO-CA không có trách nhiệm kiểm tra và đánh giá việc sử dụng chứng thư chữ ký số của người nhận;
- Chứng thư chữ ký số được sử dụng theo đúng phần mở rộng của trường KeyUsage trong chứng thư chữ ký số (Ví dụ: chữ ký số mà không có hiệu lực thì chứng thư chữ ký số không được tin cậy cho tính xác thực chữ ký của thuê bao);
- Kiểm tra trạng thái của chứng thư chữ ký số và tất cả các CA trong chuỗi tham gia phát hành chứng thư chữ ký số. Nếu bất cứ một chứng thư chữ ký số nào trong chuỗi bị thu hồi, người nhận phải chịu trách nhiệm xem xét độ tin cậy của chữ ký số do thuê bao thực hiện tại thời điểm trước khi bị thu hồi có đúng đắn không. Bất cứ tin cậy nào đưa ra đều có thể gây rủi ro tới người nhận.
- Khi sử dụng chứng thư chữ ký số hợp lý, người nhận cần sử dụng phương tiện phần mềm, phần cứng hợp lý nhằm tiến hành xác minh chữ ký số hoặc các thao tác mật mã cần thiết khác. Các thao tác này bao gồm cả việc xác định chuỗi chứng thư chữ ký số và kiểm tra các chữ ký số trên tất cả chứng thư chữ ký số trong chuỗi.

4.6 Gia hạn chứng thư chữ ký số:

4.6.1 Các trường hợp được gia hạn chứng thư chữ ký số của thuê bao:

Chỉ có các chứng thư chữ ký số đang hoạt động hợp lệ (không bị tạm dừng, thu hồi) mới có thể thực hiện yêu cầu gia hạn.

Thuê bao cần gửi yêu cầu HILO-CA gia hạn trước 30 ngày tính đến ngày hết hạn sử dụng chứng thư chữ ký số đó.

4.6.2 Đối tượng có thể yêu cầu gia hạn chứng thư chữ ký số:

Chỉ có thuê bao của HILO-CA mới có thể được gia hạn chứng thư chữ ký số.

Chỉ có thuê bao cá nhân hoặc đại diện theo pháp luật của tổ chức đối với thuê bao tổ chức mới được phép yêu cầu gia hạn chứng thư chữ ký số.

4.6.3 Xử lý yêu cầu gia hạn chứng thư chữ ký số:

Thuê bao cần tiến hành điền đủ thông tin yêu cầu trong Phiếu yêu cầu gia hạn chứng thư chữ ký số theo mẫu do HILO-CA ban hành và nộp về HILO-CA để tiến hành gia hạn.

Sau khi nhận được yêu cầu gia hạn chứng thư chữ ký số, HILO-CA tiến hành xác minh thông tin đề nghị như quy định tại phần 3.

Nếu thông tin xác thực, việc gia hạn được tiến hành. Nếu thông tin sai lệch, yêu cầu bị từ chối.

Ngoài ra, HILO-CA sẽ yêu cầu người thực hiện chứng minh mình đủ thẩm quyền để thực hiện việc gia hạn và những yêu cầu cho xác thực yêu cầu cấp chứng thư chữ ký số gốc sẽ được sử dụng để gia hạn.

4.6.4 Thông báo cho thuê bao về việc gia hạn chứng thư chữ ký số:

Việc thông báo cho thuê bao về việc phát hành chứng thư chữ ký số mới tuân theo quy định ghi tại phần 4.2

4.6.5 Xác nhận đối với chứng thư chữ ký số được gia hạn:

Điều kiện cấu thành điều khoản gia hạn chứng thư chữ ký số tuân theo phần 4.3

4.6.6 Công bố chứng thư chữ ký số đã được gia hạn:

HILO-CA có trách nhiệm công bố chứng thư chữ ký số được gia hạn trên kho lưu trữ công khai theo phần 2.

4.6.7 Thông báo chứng thư chữ ký số được gia hạn đến các đối tượng khác:

HILO-CA có trách nhiệm thông báo tới ROOT-CA, HILO-RA về việc gia hạn chứng thư chữ ký số do họ xác thực định danh.

4.7 Thay đổi cặp khóa của thuê bao:

4.7.1 Các trường hợp được thay đổi cặp khóa:

Thuê bao được thay đổi khóa trong các trường hợp sau:

- Thiết bị chứa khóa bị hư hỏng.
- Thuê bao mất thiết bị chứa khóa.
- Thuê bao/HILO-CA phát hiện khóa có dấu hiệu bị lộ.
- Thay đổi khóa theo nhu cầu sử dụng của thuê bao.
- Thuê bao thay đổi thông tin dẫn đến phải thay đổi khóa tương ứng với thông tin mới.
- Các trường hợp khác theo quy định của pháp luật.
- Thuê bao còn hạn hợp đồng hoặc gia hạn/ký mới hợp đồng mới có thể gửi yêu cầu thay đổi cặp khóa.

4.7.2 Đối tượng được gửi yêu cầu thay đổi cặp khóa:

Chỉ có thuê bao của HILO-CA mới có thể được gửi yêu cầu thay đổi cặp khóa.

Chỉ có thuê bao cá nhân hoặc đại diện theo pháp luật của tổ chức đối với thuê bao tổ chức mới được phép yêu cầu thay đổi cặp khóa.

4.7.3 Xử lý yêu cầu thay đổi cặp khóa:

Thuê bao cần tiến hành các thủ tục theo phần 4.1 và điền đủ thông tin yêu cầu trong bản Phiếu yêu cầu thay đổi khóa theo mẫu do HILO-CA ban hành.

HILO-CA hoặc HILO-CA tiến hành xác thực thông tin cung cấp của thuê bao theo phần 3.3. Nếu thông tin xác thực, việc thay khóa được tiến hành. Nếu thông tin sai lệch, yêu cầu bị từ chối.

4.7.4 Thông báo cập nhật chứng thư chữ ký số sau khi thay đổi cặp khóa:

Thông báo cho thuê bao về việc thay cặp khóa chứng thư chữ ký số theo phần 4.3.2

4.7.5 Xác nhận đối với chứng thư chữ ký số được cập nhật:

Điều khoản chấp nhận thay cặp khóa chứng thư chữ ký số theo phần 4.4.1

4.7.6 Công bố chứng thư chữ ký số được cập nhật sau khi thay đổi cặp khóa:

HILO-CA có trách nhiệm công bố chứng thư chữ ký số được thay cặp khóa trên kho lưu trữ công khai theo phần 2.2

4.7.7 Thông báo chứng thư chữ ký số được cập nhật sau khi thay đổi cặp khóa đến các đối tượng khác:

HILO-CA có trách nhiệm thông báo cho Hilo-RA và các đơn vị quản lý theo quy định về việc thay khóa chứng thư chữ ký số do họ xác thực định danh.

4.8 Thay đổi thông tin chứng thư chữ ký số:

Sửa đổi chứng thư chữ ký số là việc HILO-CA phát hành chứng thư chữ ký số mới cho thuê bao thay đổi các thông tin trong chứng thư chữ ký số ngoại trừ khóa công khai.

4.8.1 Các trường hợp được thay đổi thông tin chứng thư chữ ký số:

Thuê bao được thay đổi thông tin chứng thư chữ ký số trong các trường hợp sau:

- Phát hiện thông tin chứng thư chữ ký số không đúng thông tin của chủ thể thuê bao.
- Chủ thể thuê bao thay đổi thông tin dẫn đến phải thay đổi chứng thư chữ ký số. Các thông tin khi thay đổi phải đổi thông tin chứng thư chữ ký số được quy định tại phần 4.8

4.8.2 Đối tượng được gửi yêu cầu thay đổi thông tin chứng thư chữ ký số:

Chỉ có thuê bao của HILO-CA mới có thể được gửi yêu cầu thay thông tin chứng thư chữ ký số.

Chỉ có thuê bao cá nhân hoặc đại diện theo pháp luật của tổ chức đối với thuê bao tổ chức mới được phép yêu cầu thay đổi chứng thư chữ ký số.

Thuê bao còn hạn hợp đồng hoặc gia hạn/ký mới hợp đồng mới có thể gửi yêu cầu thay thông tin chứng thư chữ ký số.

4.8.3 Xử lý yêu cầu thay đổi thông tin chứng thư chữ ký số:

Thuê bao điền phiếu yêu cầu thay đổi thông tin chứng thư chữ ký số do HILO-CA ban hành.

HILO-CA tiến hành xác minh tính hợp lệ của thông tin yêu cầu từ thuê bao theo phần 3.2.

Quá trình xác minh trả kết quả hồ sơ hợp lệ, HILO-CA tiến hành thay cấp chứng thư chữ ký số mới cho thuê bao theo thông tin mới theo phần 4.3

4.8.4 Thông báo cập nhật cho thuê bao về việc sửa đổi chứng thư chữ ký số:

Xem phần 4.3.2

4.8.5 Xác nhận đối với chứng thư chữ ký số được cập nhật:

Xem phần 4.4.1

4.8.6 Công bố chứng thư chữ ký số được cập nhật sau khi thay đổi thông tin:

Xem phần 4.4.2

4.8.7 Thông báo chứng thư chữ ký số được cập nhật sau khi thay đổi thông tin đến các đối tượng khác:

Xem phần 4.4.3

4.9 Tạm dừng, phục hồi, thu hồi chứng thư chữ ký số:

4.9.1 Các trường hợp được phép thu hồi chứng thư chữ ký số:

Chứng thư chữ ký số của thuê bao sẽ bị thu hồi trong những trường hợp sau đây:

- Khi thuê bao yêu cầu bằng văn bản và yêu cầu này đã được tổ chức cung cấp dịch vụ chứng thực chữ ký số xác minh là chính xác;
- Khi HILO-CA phát hiện Thuê bao vi phạm nghĩa vụ trách nhiệm đối với hợp đồng hoặc các thỏa thuận đã được cam kết trước đó;
- Khi HILO-CA phát hiện thông tin trong Chứng thư chữ ký số đã được cấp ra bị sai thông tin, sai mục đích sử dụng, có dấu hiệu giả mạo;
- HILO-CA có lý do để tin rằng khóa bí mật của một trong các CA hoặc RA của HILO-CA bị xâm phạm
- Khi có yêu cầu của cơ quan Nhà nước có Thẩm quyền;
- Các điều kiện thu hồi chứng thư được quy định trong hợp đồng cung cấp dịch vụ chứng thực chữ ký số công cộng, phù hợp với quy định pháp luật.

4.9.2 Đối tượng được phép yêu cầu thu hồi chứng thư chữ ký số:

- Chủ sở hữu của chứng thư chữ ký số

(Điều kiện: Thuê bao phải còn hạn hợp đồng mới có thể gửi yêu cầu thu hồi chứng thư chữ ký số).

- Cơ quan Nhà nước có Thẩm quyền.

4.9.3 Quy trình, thủ tục thu hồi chứng thư chữ ký số:

Các Cơ quan, tổ chức có thẩm quyền gửi công văn yêu cầu việc thu hồi chứng thư chữ ký số hoặc chủ thuê bao gửi yêu cầu thu hồi chứng thư chữ ký số theo mẫu HILO-CA ban hành tới HILO-CA.

HILO-CA tiếp nhận yêu cầu thu hồi và tiến hành xác minh đề nghị thu hồi sẽ được tiến hành theo nội dung trong phần 3.4

Trường hợp kết quả trả xác minh không thành công, HILO-CA sẽ từ chối đề nghị và gửi kết quả ghi rõ lý do;

Trường hợp kết quả xác minh thành công, HILO-CA tiến hành thu hồi chứng thư chữ ký số của thuê bao.

Sau khi thu hồi, HILO-CA công bố trên cơ sở dữ liệu và gửi thông báo tới Thuê bao đính kèm lý do.

4.9.4 Thời hạn gia hạn yêu cầu thu hồi chứng thư chữ ký số:

Không có giới hạn thời gian để gửi yêu cầu thu hồi, miễn là:

- Chứng thư chữ ký số còn hiệu lực tại thời điểm gửi yêu cầu, hoặc
 - Có lý do chính đáng để thu hồi (ví dụ: khóa bị lộ, thuê bao mất khả năng sử dụng, yêu cầu từ cơ quan Nhà nước có thẩm quyền...).
- ⇒ Thuê bao có thể yêu cầu thu hồi chứng thư bất cứ lúc nào, miễn là chứng thư chưa hết hạn, hoặc việc thu hồi là cần thiết theo quy định pháp luật.

4.9.5 Thời gian phải xử lý yêu cầu thu hồi chứng thư chữ ký số:

HILO-CA tiến hành xử lý xác minh khi nhận được thông tin yêu cầu.

4.9.6 Yêu cầu kiểm tra trạng thái thu hồi chứng thư chữ ký số đối với các bên tin tưởng:

Thuê bao kiểm tra trạng thái thu hồi thông qua OCSP hoặc CRL

- OCSP: <http://ocsp.HILO-CA.vn>
- CRL: <http://crl.HILO-CA.vn/hiloca.crl>

4.9.7 Tần suất công bố danh sách thu hồi chứng thư chữ ký số(CRL):

Trong trường hợp có chứng thư chữ ký số bị thu hồi, HILO-CA sẽ công bố thông tin thu hồi trên CRL chậm nhất không quá 24 giờ kể từ thời điểm thu hồi.

4.9.8 Độ trễ công bố CRL:

CRL được phát hành công khai và quá trình này được tiến hành tự động ngay sau khi danh sách CRL được cập nhật.

4.9.9 Kiểm tra trạng thái/thu hồi chứng thư chữ ký số trực tuyến:

Kiểm tra trạng thái chứng thư chữ ký số trực tuyến (OCSP) truy cập tại địa chỉ:

- OCSP: <http://ocsp.HILO-CA.vn>
- CRL: <http://crl.HILO-CA.vn/hiloca.crl>

4.9.10 Yêu cầu kiểm tra trạng thái thu hồi chứng thư chữ ký số trực tuyến:

Thông qua OCSP Response

4.9.11 Các hình thức thông báo thu hồi khác:

HILO-CA không sử dụng các hình thức thông báo thu hồi khác ngoài các hình thức đã được nêu trong quy trình.

4.9.12 Yêu cầu đặc biệt liên quan đến thay đổi cặp khóa:

Khi khóa bí mật của HILO-CA bị mất, bị lộ hoặc có nghi ngờ bị mất/lộ, HILO-CA sẽ thực hiện các hành động sau:

- Tạm dừng việc cấp phát chứng thư chữ ký số mới.
- Thông báo cho RootCA về sự việc.
- Thực hiện theo hướng dẫn của RootCA.

4.9.13 Các trường hợp được phép tạm dừng, phục hồi chứng thư chữ ký số:

Việc tạm dừng chứng thư chữ ký số được áp dụng trong trường hợp:

- Thuê bao không bổ sung đầy đủ, chính xác giấy tờ xác minh thông tin thuê bao.
- Thuê bao không đóng đủ và đúng hạn phí thuê bao dịch vụ.

4.9.14 Đối tượng được phép yêu cầu tạm dừng chứng thư chữ ký số:

- HILO-CA là đơn vị chủ động thực hiện tạm dừng chứng thư trong các trường hợp phù hợp với chính sách quản lý chứng thư chữ ký số.

4.9.15 Quy trình, thủ tục yêu cầu tạm dừng, phục hồi chứng thư chữ ký số:

I. Tạm dừng chứng thư chữ ký số:

1. Phát hiện thiếu hồ sơ:

- Bộ phận nghiệp vụ/kiểm soát thực hiện kiểm tra định kỳ hoặc theo quy trình xử lý cấp CTS.
- Xác định trường hợp chứng thư chữ ký số đã cấp nhưng chưa thu đủ hồ sơ hợp lệ từ thuê bao.
- Gửi thông báo chính thức (qua email, văn bản hoặc hệ thống quản lý thuê bao) đến Thuê bao, nêu rõ:
 - Lý do tạm dừng.
 - Thời hạn bổ sung hồ sơ.
 - Hướng dẫn hoàn thiện hồ sơ để phục hồi Chứng thư chữ ký số.

2. Quyết định tạm dừng:

- Bộ phận phụ trách trình báo cáo sự việc lên người có thẩm quyền trong HILO-CA.
- Sau khi được phê duyệt, tiến hành thực hiện tạm dừng hiệu lực của chứng thư chữ ký số trên hệ thống.

3. Ghi nhận:

- Ghi nhận trạng thái “Tạm dừng” của chứng thư trong hệ thống quản lý CTS.

II. Phục hồi chứng thư chữ ký số:

1. Tiếp nhận và kiểm tra hồ sơ bổ sung:

- Thuê bao nộp bổ sung đầy đủ hồ sơ theo yêu cầu.
- Bộ phận nghiệp vụ xác nhận tính hợp lệ và đầy đủ của hồ sơ.

2. Quyết định phục hồi:

- Sau khi hồ sơ đạt yêu cầu, bộ phận phụ trách thực hiện phục hồi hiệu lực của chứng thư chữ ký số trên hệ thống.
- Trạng thái chứng thư chuyển từ “Tạm dừng” sang “Hoạt động”.

3. Thông báo kết quả:

- Gửi thông báo xác nhận phục hồi hiệu lực chứng thư cho thuê bao.

III. Quá thời hạn xử lý:

- Nếu sau 30 ngày kể từ ngày tạm dừng mà thuê bao không hoàn thiện hồ sơ, HILO-CA sẽ thực hiện thu hồi chứng thư theo đúng quy trình thu hồi hiện hành.
- Thuê bao sẽ nhận được thông báo về việc thu hồi và lý do.

4.9.16 Giới hạn thời hạn tạm dừng, phục hồi chứng thư chữ ký số:

Chứng thư chữ ký số bị tạm dừng, thu hồi ngay lập tức sau khi HILO-CA xác thực thông tin là hợp lệ.

Thời gian tạm dừng, phục hồi không được vượt quá thời hạn của chứng thư chữ ký số. Nếu thời gian yêu cầu tạm dừng, phục hồi quá thời hạn của chứng thư chữ ký số, HILO-CA hướng dẫn thuê bao chuyển sang yêu cầu thu hồi chứng thư chữ ký số.

4.10 Kiểm tra trạng thái chứng thư chữ ký số:

4.10.1 Các hình thức kiểm tra trạng thái chứng thư chữ ký số của thuê bao:

Thuê bao có thể kiểm tra trạng thái chứng thư chữ ký số thông qua CRL tại trang web của HILO-CA (<https://HILO-CA.vn/tra-cuu-cts/>), dịch vụ LDAP hoặc thông qua dịch vụ OCSP (nếu có thể).

4.10.2 Tính sẵn sàng của dịch vụ kiểm tra trạng thái chứng thư chữ ký số:

Dịch vụ kiểm tra trạng thái chứng thư chữ ký số luôn sẵn sàng 24/7 và không bị gián đoạn.

Trường hợp nâng cấp, bảo trì, phát sinh vấn đề cần xử lý, HILO-CA sẽ thông báo kế hoạch xử lý trên website của HILO-CA.

4.10.3 Các tính năng khác:

Dịch vụ OCSP là dịch vụ tùy chọn không cung cấp cho mọi trường hợp mà chỉ được dùng cho một số trường hợp xác định.

4.11 Chấm dứt dịch vụ của thuê bao:

4.11.1 Các trường hợp thuê bao chấm dứt dịch vụ.

Thuê bao sẽ chấm dứt quá trình sử dụng chứng thư chữ ký số trong các trường hợp sau:

- Chứng thư chữ ký số hết hạn và không đề nghị gia hạn;

- Chứng thư chữ ký số bị thu hồi trước khi hết hạn và không thay thế bằng chứng thư chữ ký số mới.

4.11.2 Thủ tục chấm dứt dịch vụ:

- Thủ tục chấm dứt dịch vụ được thực hiện tự động bởi hệ thống HILO-CA khi chứng thư chữ ký số hết hạn.

4.12 Lưu trữ và phục hồi:

Trường hợp thuê bao ủy thác cho đơn vị hoặc cá nhân khác giữ khóa phải có văn bản ký kết giữa bên ủy thác và bên được ủy thác.

4.12.1 Chính sách và thực tiễn việc lưu trữ và phục hồi khóa:

HILO-CA không có quy định.

4.12.2 Chính sách và thực tiễn việc mã hóa và phục hồi khóa phiên:

HILO-CA không có quy định.

5. KIỂM SOÁT, QUẢN LÝ VÀ VẬN HÀNH:

5.1 Kiểm soát an toàn, an ninh vật lý:

5.1.1 Vị trí đặt và xây dựng hệ thống:

Hệ thống thiết bị HILO-CA được triển khai tại hai trung tâm dữ liệu độc lập nhằm đảm bảo tính sẵn sàng cao (high availability) và khả năng khôi phục sau thảm họa (disaster recovery).

Các trung tâm dữ liệu này được lựa chọn dựa trên các tiêu chí nghiêm ngặt về an toàn, an ninh, và được trang bị nhiều lớp bảo vệ để bảo đảm mức độ an toàn vật lý và mạng cao nhất cho hệ thống HILO-CA.

5.1.2 Truy cập vật lý:

Hệ thống HILO-CA được bảo vệ bởi nhiều lớp an ninh vật lý, với sự kiểm soát chặt chẽ tại từng lớp, cụ thể:

- o **Lớp bảo vệ vòng ngoài:** Có nhân viên bảo vệ trực 24/7, kiểm soát ra vào khu vực trung tâm dữ liệu.
- o **Lớp bảo vệ khu vực đặt thiết bị:** Chỉ những cá nhân được cấp quyền truy cập mới được phép vào khu vực này.
- o **Lớp bảo vệ tủ thiết bị:** Thiết bị được đặt trong các tủ có khóa bảo mật, chỉ người được phân quyền quản trị hệ thống mới có thể truy cập.

Toàn bộ khu vực được giám sát bằng hệ thống camera an ninh hoạt động 24/7, ghi lại đầy đủ các hoạt động diễn ra trong trung tâm dữ liệu.

Quyền truy cập vật lý vào hệ thống chỉ được cấp cho những cá nhân có trách nhiệm quản trị, vận hành hoặc theo dõi hệ thống, và phải được ghi nhận trong danh sách kiểm soát truy cập của HILO-CA.

5.1.3 Điều hòa và nguồn điện:

Trung tâm vận hành HILO-CA (NOC) đặt tại vị trí trung tâm thành phố nên điều kiện về nguồn điện được đảm bảo tốt. Hệ thống HILO-CA đi vào vận hành sẽ hoạt động với độ ổn định cao nên việc sử dụng phòng NOC cũng ít xảy ra. Trường hợp sử dụng gấp, nhân sự vận hành hệ thống đăng ký và thực hiện trực tiếp tại DC/DRC.

Phòng NOC được trang bị hệ thống điều hòa và hạn chế tối đa thiết bị nhằm giảm thiểu nguy cơ cháy nổ có thể xảy ra.

Hệ thống thiết bị chính của HILO-CA đặt tại trung tâm dữ liệu của Viettel (IDC Viettel Láng Hòa Lạc) và FPT (IDC FPT 17 Duy Tân).

Hai trung tâm dữ liệu đáp ứng đầy đủ điều kiện về nguồn điện, điều hòa, phòng chống cháy nổ... đảm bảo hệ thống HILO-CA vận hành ổn định và liên tục 24/7

5.1.4 Tiếp xúc với nước:

Hệ thống thiết bị được bố trí hạn chế tiếp xúc tối đa với nước

5.1.5 Phòng ngừa và bảo vệ chống cháy:

Tuân thủ các biện pháp phòng cháy cháy nổ

Có phương án phòng ngừa để ngăn chặn và dập tắt lửa hay các thảm họa khác có thể gây cháy hoặc khói.

5.1.6 Phương tiện lưu trữ:

Tất cả các sản phẩm lưu trữ thông tin về phần mềm và dữ liệu, kiểm toán, tư liệu hay thông tin dự phòng được lưu trữ đảm bảo an ninh thông qua các triển khai an ninh vật lý và điều khiển truy cập nhằm ngăn ngừa truy cập trái phép và bảo vệ phương tiện lưu trữ không bị phá hủy (do nước, lửa, điện từ trường...)

5.1.7 Xử lý rác:

Tài liệu giấy: Các tài liệu và tài nguyên nhạy cảm được cắt vụn, đảm bảo không thể khôi phục.

Tài liệu điện tử: Các phương tiện thu thập hay truyền thông tin nhạy cảm được xử lý để đảm bảo các thông tin này không bị truy cập bất hợp pháp trước khi tiêu hủy.

Các thiết bị dùng để mã hóa phải được phá hủy về mặt vật lý theo hướng dẫn của nhà sản xuất.

5.1.8 Hệ thống dự phòng:

Hệ thống dự phòng (DRC) HILO-CA đặt tại trung tâm dữ liệu IDC Viettel tại Láng Hòa Lạc.

Hệ thống dự phòng cách hệ thống chính (IDC FPT 17 Duy Tân) trên 30km nên đảm bảo điều kiện khoảng cách tối thiểu hai hệ thống.

HILO-CA xây dựng hệ thống dự phòng có thiết kế gần giống với hệ thống chính. Hệ thống chính và dự phòng kết nối với nhau qua kênh truyền riêng và có cơ chế back up dữ liệu đảm bảo hệ thống dự phòng có thể hoạt động nhanh nhất thay thế hệ thống chính khi có sự cố xảy ra.

5.2 Kiểm soát quy trình:

5.2.1 Các vai trò đáng tin cậy:

Nhân viên kỹ thuật, nhân viên vận hành đều phải được xem xét trước khi trở thành người tin cậy làm việc tại vị trí được tin cậy của HILO-CA. Những người được chọn là người tin cậy làm việc tại vị trí tin cậy đáp ứng yêu cầu của HILO-CA.

Người tin cậy bao gồm tất cả các nhân viên, kỹ sư, nhân viên vận hành có truy cập hay điều khiển quá trình xác thực hoặc mã hóa có thể gây ảnh hưởng lớn tới:

- Quá trình kiểm tra thông tin trong ứng dụng chứng thư chữ ký số;
- Quá trình cung cấp dịch vụ chứng thực chữ ký số;
- Ban hành, thu hồi quyền truy cập tới các phần bị hạn chế của hệ thống;
- Chuyển giao thông tin hoặc yêu cầu của thuê bao.

Người tin cậy bao gồm, nhưng không giới hạn bởi các thành phần sau:

- Nhân viên giao dịch, nhân viên chăm sóc khách hàng;
- Nhân viên điều hành công việc mã hóa;
- Nhân viên an ninh;
- Nhân viên bảo mật hệ thống;

- Các kỹ sư thiết kế;

Hilo-CA thiết lập, duy trì và có các yêu cầu nghiêm ngặt về thủ tục điều khiển để đảm bảo quá trình phân công nhiệm vụ dựa trên khả năng làm việc và đảm bảo rằng nhiều người tin cậy sẽ cùng thực hiện các công việc có tính bảo mật cao.

Chính sách và thủ tục được thực hiện để đảm bảo sự phân công nhiệm vụ dựa trên khả năng làm việc. Những công việc mang tính nhạy cảm cao, chẳng hạn truy cập và quản lý hệ thống phần cứng mã hóa và các công việc liên quan đến khóa, yêu cầu nhiều người tin cậy tham gia.

Những thủ tục điều khiển ở bên trong được thiết kế để đảm bảo ít nhất hai người tin cậy cùng tham gia truy cập tới mức vật lý hoặc mức logic của thiết bị. Truy cập tới phần cứng mã hóa yêu cầu chặt chẽ phải có nhiều người tin cậy cùng tham gia toàn bộ quá trình làm việc, từ việc nhận và kiểm tra cho tới bước cuối cùng là hủy về logic và/hoặc về vật lý. Mỗi một lần modul này được kích hoạt trong các thao tác liên quan đến khóa, các truy cập xa hơn nữa sẽ bị thu hồi để duy trì việc phân cách giữa điều khiển các truy cập ở mức vật lý và mức logic tới thiết bị. Những người có truy cập vật lý tới các module không giữ thông tin cho phép truy cập vào hệ thống và ngược lại.

5.2.2 Số lượng người cần thiết cho mỗi công việc:

HILO-CA thiết lập, duy trì và có các yêu cầu nghiêm ngặt về thủ tục điều khiển để đảm bảo sự phân công nhiệm vụ dựa trên khả năng làm việc.

Các chính sách và thủ tục kiểm soát này của HILO-CA luôn đòi hỏi có ít nhất 2 người để thực hiện các công việc nhạy cảm.

5.2.3 Định danh và xác thực trong mỗi thành viên:

Tất cả mọi đối tượng muốn trở thành người tin cậy, quy trình xác thực định danh được thực hiện với sự hiện diện về mặt con người (vật lý) của đối tượng này trước khi quy trình kiểm tra thông thường bắt đầu (như kiểm tra Căn cước, căn cước công dân, hộ chiếu, ...). Quá trình xác thực định danh được thực hiện thêm một lần nữa thông qua thủ tục kiểm tra lý lịch.

HILO-CA đảm bảo những nhân viên đạt được vị trí được tin cậy và trao quyền cho các nhân viên này:

- Được cấp phép truy cập tới các phạm vi cần thiết;

- Được cấp tài liệu điện tử để có thể truy cập đến và thực hiện một số chức năng trên HILO-CA, Hilo-RA hay các hệ thống công nghệ thông tin khác.

5.2.4 Vai trò, trách nhiệm của từng thành viên:

HILO-CA đảm bảo những nhân viên đạt được vị trí được tin cậy và trao quyền cho các nhân viên này:

- Được cấp phép truy cập tới các phạm vi cần thiết;
- Được cấp tài liệu điện tử để có thể truy cập đến và thực hiện một số chức năng trên HILO-CA, Hilo-RA hay các hệ thống công nghệ thông tin khác.

Các vai trò cần phải có sự phân tách nhiệm vụ, bao gồm nhưng không giới hạn:

- Xác minh thông tin hồ sơ cấp Chứng thư chữ ký số
- Các nghiệp vụ liên quan tới vòng đời chứng thư chữ ký số
- Quản lý thông tin, yêu cầu thuê bao.

5.3 Kiểm soát nhân sự:

HILO-CA có các tài liệu về kiểm soát nhân sự và chính sách bảo mật cho HILO-CA và Hilo-RA. Việc tuân thủ những chính sách bao gồm các yêu cầu kiểm tra độc lập được mô tả ở phần 8. Những tài liệu này chứa thông tin bảo mật nhạy cảm và chỉ dành riêng cho bên tham gia dịch vụ HILO-CA dưới sự đồng ý của HILO-CA.

5.3.1 Kinh nghiệm, bằng cấp, chứng chỉ của đội ngũ nhân sự liên quan đến quản lý và vận hành hệ thống:

Trước khi chứng nhận vai trò được tin cậy cho một nhân viên, HILO-CA thực hiện việc kiểm tra lý lịch gồm các yếu tố sau:

- Giấy xác nhận của địa phương về cá nhân, gia đình;
- Xác nhận của đơn vị công tác trước đó;
- Kiểm tra, tham khảo từ các đồng nghiệp;
- Kiểm tra các tiền án, tiền sự ở địa phương cũng như cấp quốc gia;
- Xác nhận đáp ứng các điều kiện về chính trị và an ninh của cơ quan chính trị và bảo vệ an ninh của HILO-CA.

Khi một trong các yếu tố bắt buộc này không thể đạt được do luật pháp hoặc hoàn cảnh nào đó, HILO-CA sẽ sử dụng kỹ thuật đánh giá thay thế khác được luật pháp cho phép.

5.3.2 Quy trình kiểm tra lý lịch:

HILO-CA kiểm tra các thông tin sau, trước khi bổ nhiệm vào vai trò tin tưởng:

- Kiểm tra, xác minh thông tin theo sơ yếu lý lịch.
- Xác minh trình độ học vấn cao nhất đạt được.

Báo cáo bao gồm các thông tin trên được bộ phận quản trị nguồn nhân lực và các nhân viên an ninh đánh giá, từ đó đưa ra các biện pháp thích hợp cho mỗi tình huống. Các biện pháp này có thể bao gồm việc kiểm tra và loại bỏ ứng viên khỏi vị trí được tin cậy hoặc chấm dứt công việc của ứng viên.

Việc sử dụng các thông tin thu thập được từ trong quá trình kiểm tra lý lịch phải phù hợp với luật pháp và chính sách của nhà nước.

Các yếu tố phát hiện được trong quá trình kiểm tra lý lịch có thể dùng để loại bỏ ứng viên thông thường là:

- Thông tin do ứng viên hoặc người tin cậy cung cấp không trung thực;
- Mức độ không tán thành hay tin tưởng cao của người tin cậy;
- Có tiền án tiền sự;
- Thiếu khả năng hoặc có dấu hiệu không minh bạch về tài chính.

5.3.3 Yêu cầu về đào tạo cho cán bộ vận hành, quản lý hệ thống:

HILO-CA đào tạo nhân viên sau tuyển dụng cũng như trong quá trình làm việc để đảm bảo nhân viên có thể hoàn thành công việc của mình.

HILO-CA sẽ lưu giữ các tư liệu của những lần đào tạo này đồng thời thường xuyên xem xét lại và nâng cấp các chương trình đào tạo khi thấy cần thiết.

Chương trình đào tạo của HILO-CA thích hợp cho mỗi công việc riêng lẻ và thường liên quan tới:

- Các vấn đề cơ bản của hạ tầng khóa công khai;
- Yêu cầu công việc;
- Chính sách, thủ tục an ninh và các hoạt động của HILO-CA;

- Sử dụng và điều hành các thiết bị phần cứng, phần mềm đã triển khai;
- Báo cáo, chuyển giao các thỏa ước và các vấn đề liên quan;
- Thủ tục khôi phục sau thảm họa và duy trì công việc.

Chương trình đào tạo của HILO-CA được thiết kế tương thích với chương trình đào tạo về chữ ký số và chứng thực chữ ký số do Trung tâm Chứng thực điện tử quốc gia (NEAC) cung cấp.

Ngoài ra, HILO-CA sẽ thường xuyên tham gia các hội thảo về chữ ký số, an toàn bảo mật tại Việt nam và các diễn đàn trên thế giới.

HILO-CA khuyến khích cán bộ thi thêm các chứng chỉ, bằng cấp liên quan đến chứng thư chữ ký số và an toàn bảo mật thông tin.

5.3.4 Tần suất và yêu cầu đào tạo lại:

Trong quá trình làm việc, các nhân viên trong hệ thống HILO-CA sẽ thường xuyên được đào tạo nâng cao chuyên môn. Thời gian đào tạo do đơn vị quản lý quyết định dựa theo yêu cầu để mỗi nhân viên cần để duy trì mức độ tin tưởng và thực hiện tốt các công việc của bản thân.

5.3.5 Tần suất và trình tự luân chuyển công việc:

HILO-CA không quy định.

5.3.6 Các hình thức xử lý đối với hành động không được phép:

Các biện pháp kỉ luật phù hợp được thi hành đối với các hành vi bất hợp pháp hay các hành vi vi phạm chính sách, quy định của HILO-CA. Các biện pháp kỉ luật có thể bao gồm việc sa thải tùy thuộc vào tần suất và mức độ nghiêm trọng của các hành vi nêu trên. Các yêu cầu ký kết độc lập

Trong một số trường hợp nhất định, các nhân viên triển khai hay tư vấn độc lập được sử dụng vào các vị trí tin cậy. Những nhân viên này có cùng chức năng và vai trò an ninh như các nhân viên HILO-CA ở vị trí tương ứng.

Các đối tượng trên phải là người đã hoàn thành hay vượt qua thủ tục kiểm tra lý lịch và được phép truy cập tới các phương tiện được bảo mật của dịch vụ HILO-CA trong phạm vi quyền hạn của họ.

Các trường hợp khác hình thức xử lý các trường hợp vi phạm theo quy định của pháp luật có liên quan và thỏa thuận.

5.3.7 Yêu cầu đối với nhà thầu độc lập:

Các nhà thầu độc lập hoặc bên thứ ba khi tham gia vào việc cung cấp dịch vụ, triển khai, bảo trì hoặc hỗ trợ kỹ thuật cho HILO-CA phải tuân thủ các yêu cầu sau:

- Ký cam kết bảo mật thông tin theo mẫu do HILO-CA ban hành.
- Chỉ được phép truy cập vào các khu vực hoặc hệ thống theo đúng phạm vi công việc đã được HILO-CA phê duyệt.
- Chịu sự giám sát của nhân sự HILO-CA trong suốt quá trình làm việc tại các khu vực nhạy cảm.
- Không được phép sao chép, thu thập, hoặc lưu trữ bất kỳ dữ liệu, thông tin nào thuộc về HILO-CA nếu không có sự cho phép bằng văn bản.
- Phải được đào tạo hoặc hướng dẫn đầy đủ về quy trình an toàn – bảo mật trước khi tiếp cận hệ thống.

5.3.8 Cung cấp tài liệu cho nhân viên:

HILO-CA đảm bảo rằng tất cả nhân viên có liên quan đến hoạt động vận hành hệ thống chứng thực số được:

- Cung cấp đầy đủ các tài liệu hướng dẫn, quy trình nội bộ, chính sách an toàn thông tin và chính sách vận hành hệ thống.
- Được đào tạo định kỳ về các nội dung liên quan đến trách nhiệm công việc, bảo mật thông tin, và các quy định pháp lý liên quan đến dịch vụ chứng thực chữ ký số.
- Tiếp cận tài liệu phiên bản mới nhất thông qua hệ thống quản lý tài liệu nội bộ.
- Cam kết tuân thủ các hướng dẫn trong tài liệu thông qua các hình thức như ký xác nhận, kiểm tra sau đào tạo, ...

5.4 Các quy trình ghi nhật ký hệ thống:

5.4.1 Các loại sự kiện được ghi lại:

Các sự kiện có thể kiểm định phải được ghi lại bởi HILO-CA và các Hilo-RA. Mọi bản ghi điện tử hay bằng tay, chứa thời gian của sự kiện, và nhận dạng của đơn vị thực hiện. HILO-CA đưa ra các loại bản ghi sự kiện trong CPS này.

Các dạng sự kiện được ghi tự động tại file log hệ thống trên máy chủ FileServer bao gồm:

- Các sự kiện tới hệ thống:
 - o Tạo khóa CA;
 - o Bật tắt các hệ thống và ứng dụng;
 - o Thay đổi khóa CA;
 - o Sự kiện có liên quan đến quản lý chu kỳ mã hóa;
 - o Quá trình xử lý dữ liệu kích hoạt cho khóa bí mật của CA, các bản ghi truy cập vật lý;
 - o Bảo trì và thay đổi cấu hình hệ thống;
 - o Bản ghi hủy bỏ các phương tiện chứa khóa, dữ liệu kích hoạt, hoặc thông tin thuê bao.
- Các sự kiện về vòng đời của chứng thư chữ ký số, bao gồm: phát hành, cấp lại, cấp mới, thu hồi, tạm dừng;
- Sự kiện liên quan tới người tin cậy, bao gồm:
 - o Hành động truy cập hay thoát ra;
 - o Tạo và xóa bỏ mật khẩu hay thay đổi đặc quyền của người sử dụng;
 - o Thay đổi nhân sự;
- Báo cáo về việc truy nhập vào mạng và các hệ thống không được cấp quyền;
- Lỗi trong việc đọc và ghi chứng thư chữ ký số và kho lưu trữ;
- Thay đổi chính sách tạo chứng thư chữ ký số, thời gian hợp lệ;
- Lỗi phát sinh liên quan đến chứng thư chữ ký số và dịch vụ chứng thực chữ ký số do thuê bao thông báo hoặc do HILO-CA phát hiện.

5.4.2 Tần xuất xử lý nhật ký hệ thống:

Các bản ghi nhật ký được kiểm tra tối thiểu hàng tuần đối với các sự kiện an ninh và vận hành quan trọng. Ngoài ra, HILO-CA sẽ tiến hành kiểm tra bất thường dựa theo các cảnh báo và hiện tượng của hệ thống.

5.4.3 Thời gian lưu trữ nhật ký hệ thống:

Bản ghi nhật ký kiểm tra phải được lưu trữ theo phần 5.5.2;

5.4.4 Bảo vệ nhật ký hệ thống:

- Dạng giấy(bản cứng): Lưu trong tủ hồ sơ.

- Dạng dữ liệu: Được lưu tại máy chủ có thẩm quyền và được sao lưu hàng ngày.

Nhật ký được bảo vệ với trước các hành động xem, thay đổi, xóa hay các tác động khác mà không được phép.

Dữ liệu nhật ký không có chứa bất kỳ thông tin nhạy cảm như mật khẩu người dùng. Các tham số nhạy cảm được lưu trữ dưới dạng được bảo vệ đảm bảo tính toàn vẹn và an toàn

Quản trị viên đặc quyền mới có thể thực hiện chức năng khôi phục từ các bản sao lưu.

5.4.5 Quy trình sao lưu nhật ký hệ thống:

Hàng ngày, các bản ghi kiểm tra sẽ được sao lưu những phần thay đổi, bổ sung; và hàng tuần sẽ được sao lưu dự phòng toàn bộ.

5.4.6 Hệ thống thu thập nhật ký hệ thống:

Kiểm tra hệ thống tự động được thực hiện ở mức ứng dụng, mạng và hệ điều hành. Nhân viên chuyên trách của HILO-CA sẽ thực hiện thao tác kiểm tra thủ công.

5.4.7 Thông báo cho đối tượng gây ra sự kiện:

Khi một sự kiện được ghi nhật ký, không có thông báo cho đối tượng gây ra sự kiện đó.

5.4.8 Đánh giá lỗ hổng bảo mật:

Dữ liệu nhật ký sẽ được đưa vào phân tích, kết quả phân tích sẽ cho biết các lỗ hổng tiềm tàng trong hệ thống, từ đó có phương án khắc phục.

5.5 Lưu trữ các bản ghi:

5.5.1 Các loại bản ghi được lưu trữ:

HILO-CA sẽ lưu trữ các thông tin sau

- Các dữ liệu kiểm tra trong phần 5.4;
- Thông tin đăng ký cấp chứng thư chữ ký số;
- Các tài liệu, văn bản kèm theo Phiếu yêu cầu cấp chứng thư chữ ký số;
- Thông tin về vòng đời chứng thư chữ ký số;
- Và các thông tin khác theo quy định của RootCA;

5.5.2 Thời hạn lưu trữ bản ghi:

Các dữ liệu sẽ được lưu trong một khoảng thời gian ít nhất 5 năm kể từ ngày chứng thư chữ ký số hết hạn hoặc bị hủy bỏ.

5.5.3 Bảo vệ bản ghi lưu trữ:

Phương tiện lưu trữ dữ liệu thường xuyên được bảo trì và quản lý, luôn sẵn sàng phục vụ truy cập.

5.5.4 Quy trình sao lưu bản ghi:

HILO-CA sao lưu tăng cường các thông tin chứng thư chữ ký số hàng ngày và sao lưu toàn bộ hàng tuần. Các bản sao tài liệu văn bản giấy được lưu tại địa điểm an toàn.

5.5.5 Yêu cầu về gắn dấu thời gian cho bản ghi:

Các bản ghi thông tin về chứng thư chữ ký số, CRL và các sự kiện thu hồi cần ghi lại thời gian xảy ra sự kiện.

Thông tin thời gian không được mã hóa.

5.5.6 Hệ thống thu thập bản ghi:

Hệ thống lưu trữ của HILO-CA là tập trung.

5.5.7 Quy trình truy cập và xác minh thông tin bản ghi:

Chỉ nhân sự tin tưởng được cấp phép bởi HILO-CA mới có khả năng truy cập và sử dụng dữ liệu lưu trữ.

Thông tin lưu trữ sẽ được kiểm tra tính toàn vẹn khi được lấy ra.

5.6 Thay đổi cặp khóa:

Chứng thư chữ ký số của HILO-CA có thể gia hạn với điều kiện tổng thời gian sử dụng của cặp khóa không được vượt qua thời hạn sử dụng tối đa do pháp luật quy định. Cặp khóa mới của HILO-CA có thể sinh ra khi cần thiết, ví dụ như thay thế cặp khóa cũ đã ngừng sử dụng.

Trước khi chứng thư chữ ký số của HILO-CA hết hạn, HILO-CA sẽ tiến hành quy trình gia hạn nhằm đảm bảo hệ thống hoạt động thông suốt. HILO-CA sẽ xin gia hạn chứng thư chữ ký số từ NEAC không chậm hơn 90 ngày trước thời điểm hết hạn.

Quá trình chuyển tiếp khóa của HILO-CA từ cặp khóa cũ sang cặp khóa mới đảm bảo rằng:

- Tại thời điểm nhất định trước khi hết hạn đồng thời tại thời điểm cấp khóa hết hạn, HILO-CA ban hành chứng thư chữ ký số theo quy định của pháp luật.

- HILO-CA sử dụng cấp khóa mới để ban hành chứng thư chữ ký số cho thuê bao khi nhận được yêu cầu ban hành chứng thư chữ ký số sau thời điểm tạm dừng ban hành chứng thư chữ ký số trên.

CA tiếp tục ký lên CRL bằng cấp khóa cũ đến khi nào hết hạn toàn bộ chứng thư chữ ký số được ban hành bởi cấp khóa cũ.

HILO-CA tiếp tục sử dụng cấp khóa cũ đến khi nào hết hạn toàn bộ chứng thư chữ ký số được ban hành bởi cấp khóa cũ.

5.7 Xử lý sự cố, thảm họa và phục hồi:

5.7.1 Quy trình xử lý sự cố và thảm họa:

Việc dự phòng và sao lưu cần tiến hành tại địa điểm, thiết bị khác nhằm phòng ngừa khả năng sự cố.

Khi có sự cố, các dữ liệu được phục hồi theo các thủ tục được ban hành.

Các dữ liệu cần sao lưu gồm:

- Dữ liệu đăng ký chứng thư chữ ký số;
- Dữ liệu kiểm tra, cơ sở dữ liệu của các chứng thư chữ ký số đã phát hành;
- Dữ liệu về nhật ký;
- Các bản ghi chứng thư chữ ký số được tạo ra.

Sao lưu dự phòng khóa bí mật của CA tuân theo quy định trong phần 6.2.5

5.7.2 Sự cố về tài nguyên máy tính, phần mềm và dữ liệu:

Khi xảy ra sự cố đối với tài nguyên máy tính, gồm phần cứng, phần mềm, dữ liệu, các thông tin cần gửi ngay tới đơn vị chuyên trách xử lý sự cố nhằm thực hiện quy trình xử lý đã dự tính. Trong trường hợp cần thiết, chức năng phục hồi sau sự cố sẽ được kích hoạt sử dụng.

5.7.3 Quy trình xử lý khóa bí mật bị xâm phạm:

Khi nghi ngờ, phát hiện sự cố bị lộ khóa bí mật của HILO-CA, đơn vị xử lý sự cố của HILO-CA (Incident Response Team) sẽ chuyên trách xử lý bằng các thủ tục, quy trình đã dự tính. Nhân sự của đơn vị xử lý sự cố bao gồm chuyên gia về mật mã, an ninh, kinh doanh, vận hành hệ thống và các chức năng khác sẽ khảo sát hiện trạng, đề ra phương án

giải quyết và triển khai kế hoạch hành động sau khi được đơn vị quản lý điều hành của HILO-CA chấp thuận.

Nếu chứng thư chữ ký số của HILO-CA bị thu hồi, các thủ tục sau cần thực hiện:

- Trạng thái thu hồi chứng thư chữ ký số của HILO-CA sẽ được công bố trên kho lưu trữ;
- Mọi biện pháp thông báo có thể có đều được sử dụng nhằm cung cấp thông tin về sự kiện thu hồi chứng thư chữ ký số CA cho các đơn vị thuộc hệ thống của HILO-CA;
- HILO-CA sinh cặp khóa mới theo quy định ở phần 4.6, ngoại trừ trường hợp HILO-CA bị ngừng hoạt động theo điều khoản trong phần 4.8.

5.7.4 Khả năng phục hồi hoạt động sau thảm họa:

HILO-CA xây dựng hệ thống dự phòng cách vị trí hệ thống chính thức tối thiểu 30 km. HILO-CA sẽ lập kế hoạch, triển khai và thử nghiệm phương án phục hồi sau sự cố nhằm giảm tối đa các hậu quả gây ra do yếu tố tự nhiên hay con người. Kế hoạch này thường xuyên được kiểm tra, xem xét và cập nhật cho phù hợp với tình hình thực tế.

Khi có sự cố do yếu tố tự nhiên hay con người gây ra làm ngừng hoạt động hệ thống tạm thời hoặc kéo dài, đơn vị giải quyết tình trạng khẩn cấp của HILO-CA (HILO-CA Emergency Response Team) có nhiệm vụ thực hiện quy trình phục hồi sau sự cố.

HILO-CA có khả năng phục hồi các hoạt động cơ bản sau 24 (hai mươi bốn) giờ sau sự cố với mức tối thiểu sau:

- Phát hành chứng thư chữ ký số;
- Thu hồi chứng thư chữ ký số;
- Công bố thông tin thu hồi.

Cơ sở dữ liệu dùng cho phục hồi sau sự cố được đồng bộ với hệ thống đang vận hành trong khoảng thời gian cho phép. Các thiết bị sử dụng cho kế hoạch phục hồi được bảo vệ theo quy định ở phần 5.1.

HILO-CA bảo quản các thiết bị phần cứng và sao lưu dự phòng tại khu vực quản lý trang thiết bị phục hồi sau sự cố. Khóa bí mật của HILO-CA được sao lưu vào bảo quản cho nhiệm vụ phục hồi sau thảm họa theo quy định ở phần 6.2.

5.8 Dừng hoạt động cung cấp dịch vụ:

HILO-CA sẽ thông báo khi HILO-CA hoặc một Hilo-RA chấm dứt hoạt động cho các đối tác, thuê bao bằng các phương tiện truyền thông hợp lý có thể sử dụng. Khi chấm dứt hoạt động, HILO-CA sẽ thực hiện quy trình chấm dứt nhằm giảm thiểu các thiệt hại tới thuê bao, người nhận. Quy trình này có thể bao gồm các bước sau:

- Cung cấp thông tin về tình trạng chấm dứt hoạt động của HILO-CA cho thuê bao và người nhận;
- Chịu chi phí cho các thông báo này;
- Thực hiện các thủ tục cần thiết nhằm thu hồi chứng thư chữ ký số của HILO-CA.
- Tiếp tục duy trì hệ thống lưu trữ các thông tin của HILO-CA theo quy định của CPS này;
- Tiếp tục duy trì hệ thống hỗ trợ dịch vụ cho thuê bao;
- Tiếp tục duy trì hệ thống dịch vụ thu hồi, như CRL, OCSP.
- Tiến hành thu hồi các chứng thư chữ ký số chưa bị thu hồi nếu thấy cần thiết.
- Hoàn phí cho thuê bao nếu chưa kết thúc hợp đồng;
- Hủy khóa bí mật của HILO-CA và các thiết bị token chứa khóa bí mật.
- Chuyển giao dịch vụ HILO-CA cho đơn vị khác nếu có.

6. ĐẢM BẢO AN TOÀN AN NINH VỀ KỸ THUẬT:

6.1 Tạo và phân phối khóa:

6.1.1 Cách thức tạo cặp khóa:

Quá trình sinh cặp khóa cho HILO-CA được thực hiện bởi những người tin cậy, tiến hành trên các hệ thống an toàn và đảm bảo tính mật mã bền vững cho cặp khóa sinh ra. Thủ tục sinh khóa sẽ được ghi lại, lưu thời gian thực hiện và ký xác nhận của tất cả những người tham gia. Các dữ liệu này được lưu trữ, kiểm tra và theo dõi trong khoảng thời gian thích hợp do HILO-CA quyết định.

Yêu cầu tối thiểu cho thiết bị mật mã sinh và lưu trữ khóa phải đạt tiêu chuẩn FIPS 140-2 level 3 theo Thông tư 06/2015/TT-BTTTT ngày 23/03/2015. Các khóa của HILO-CA được sinh và lưu trữ trong các thiết bị mật mã phần cứng này và phải sao lưu dự phòng. Khóa gốc của HILO-CA có thể dùng cho ký chứng thư chữ ký số, CRL và ký ngoại tuyến danh sách chứng thư chữ ký số bị thu hồi.

Cặp khóa của HILO-CA được đặt tại môi trường bảo vệ an toàn có phương án sao lưu và phục hồi khóa.

Cặp khóa của thuê bao được sinh ra tại PKI Smartcard, PKI token theo tiêu chuẩn FIPS 140-2 Level 2 trở lên, sử dụng sinh khóa ký số phải có Token và mã PIN xác thực truy xuất vào thiết bị.

Trong một số trường hợp khách hàng có nhu cầu đặt biệt, khách hàng sử dụng thiết bị HSM đạt chuẩn FIPS 140-2 Level 3, cặp khóa được sinh ra trong thiết bị HSM của khách hàng.

6.1.2 Chuyển giao khóa bí mật:

Khi thuê bao tự thực hiện sinh cặp khóa và gửi khóa công khai tới HILO-CA trong đăng ký chứng thư chữ ký số, việc phân phối khóa bí mật tới thuê bao là không cần thiết.

6.1.3 Chuyển giao khóa công khai cho tổ chức phát hành chứng thư chữ ký số:

Thuê bao gửi khóa công khai tới HILO-CA thông qua phương tiện điện tử được quy định theo chuẩn yêu cầu chứng thư chữ ký số PKCS#10 CSR hoặc phải bảo vệ đường truyền gói dữ liệu đã ký gửi đi theo chuẩn SSL. Khi cặp khóa được HILO-CA tạo, điều kiện này là không cần thiết.

6.1.4 Chuyển giao khóa công khai của tổ chức phát hành chứng thư chữ ký số cho bên tin tưởng:

Các bên tin cậy có thể tải và cài đặt khóa công khai của HILO-CA, RootCA từ website của HILO-CA.

Việc gửi khóa này cũng thông qua một phiên SSL để đảm bảo an ninh.

6.1.5 Kích thước khóa:

HILO-CA cấp độ dài cặp khóa tối thiểu 2048 bits

6.1.6 Tạo các tham số cho khóa công khai và kiểm tra chất lượng:

Quá trình sinh khóa công khai tuân theo chuẩn PKCS #1, đáp ứng theo các tiêu chuẩn tại Thông tư 06/2015/TT-BTTTT ngày 23/3/2015 của Bộ Thông tin và Truyền thông(Nay là Bộ Khoa học và Công nghệ) về việc Quy định Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số và Thông tư số 16/2019/TT-BTTTT ngày 05/12/2019 của Bộ Thông tin và Truyền thông(Nay là Bộ Khoa học và Công nghệ) về việc Quy định Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số trên thiết bị di động và ký số từ xa

6.1.7 Mục đích sử dụng khóa:

Mục đích sử dụng khóa được quy định các giá trị của trường “Key Usage” trong chứng thư chữ ký số X.509 phiên bản 3 phải tuân theo quy định trong RFC 5280

Phần mở rộng có thể bao gồm các thông tin sau: digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign, CRLSign, encipherOnly, decipherOnly

6.2 Kiểm soát và bảo vệ khóa bí mật, mô-đun mật mã:

HILO-CA triển khai giải pháp tích hợp về vật lý, logic và thủ tục nhằm đảm bảo tính an toàn cho khóa bí mật của HILO-CA.

Thuê bao được yêu cầu ký cam kết thực hiện các biện pháp cần thiết nhằm chống lại nguy cơ mất, để lộ, sửa đổi hoặc sử dụng trái phép khóa bí mật của thuê bao.

6.2.1 Tiêu chuẩn và kiểm soát đối với mô-đun mật mã:

HILO-CA sử dụng thiết bị mật mã phần cứng để sinh khóa và lưu trữ khóa bí mật gốc của CA. Thiết bị HILO-CA sử dụng đạt tiêu chuẩn tối thiểu như sau:

- Ký hiệu tiêu chuẩn: FIPS PUB 140-2 Level 3
- Khóa của khách hàng ký số Remote Signing được lưu trong thiết bị HSM đạt chuẩn EN 419 221-5.
- Tên đầy đủ của tiêu chuẩn: Security Requirements for Cryptographic Modules

6.2.2 Kiểm soát đa bên đối với khóa bí mật(n out of m):

Cơ chế kiểm soát khóa bí mật của HILO-CA là cơ chế chia sẻ mã theo chuẩn quốc tế, cơ chế này tách dữ liệu kích hoạt khóa bí mật thành các phần khác nhau (n), các phần được giữ bởi các đối tượng khác nhau.

Để kích hoạt khóa cần ít nhất một số lớn hơn 1 (m) mảnh khóa ($m \leq n$).

Tại HILO-CA, $m \geq 2$.

6.2.3 Chuyển giao khóa bí mật:

Khóa ký người dùng được lưu an toàn trong thiết bị HSM đạt chuẩn EN 419 221-5 đáp ứng quy định tại Thông tư số 16/2019/TT-BTTTT ngày 05/12/2019 của Bộ Thông tin và Truyền thông(Nay là Bộ Khoa học và Công nghệ) về việc Quy định Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số trên thiết bị di động và ký số từ xa

6.2.4 Dự phòng khóa bí mật:

Cặp khóa bí mật của HILO-CA được sao lưu dự phòng trên thiết bị phần cứng an toàn và được đặt cách xa vị trí lưu trữ bản chính tối thiểu 30 km.

6.2.5 Lưu trữ khóa bí mật:

Khi chứng thư chữ ký số hết hạn, cặp khóa của HILO-CA được lưu trữ an toàn trong vòng ít nhất 5 năm tiếp theo trên thiết bị mật mã phần cứng theo tiêu chuẩn do Bộ Thông tin và Truyền thông(Nay là Bộ Khoa học và Công nghệ) ban hành. Cặp khóa này không được sử dụng vào bất cứ hoạt động ký xác nhận nào sau thời gian hết hạn, trừ khi chứng thư chữ ký số của HILO-CA được gia hạn.

6.2.6 Chuyển khóa bí mật vào hoặc ra khỏi Mô-đun mật mã:

Quy trình chuyển khóa bí mật vào thiết bị mật mã an toàn được tiến hành theo hướng dẫn của nhà cung cấp thiết bị, theo chuẩn do Bộ Thông tin và Truyền thông(Nay là Bộ Khoa học và Công nghệ) ban hành

6.2.7 Lưu trữ khóa bí mật trên Mô-đun mật mã:

Quy trình lưu trữ khóa bí mật vào thiết bị mật mã an toàn được tiến hành theo hướng dẫn của nhà cung cấp thiết bị, theo chuẩn do Bộ Thông tin và Truyền thông(Nay là Bộ Khoa học và Công nghệ) ban hành

6.2.8 Phương thức kích hoạt khóa bí mật:

Tất cả các thành phần tham gia HILO-CA cần phải bảo vệ dữ liệu dùng cho kích hoạt khóa bí mật khỏi bị mất, đánh cắp, sửa đổi, để lộ hoặc sử dụng trái phép.

HILO-CA sẽ thống nhất với thuê bao phương pháp kích hoạt sử dụng khóa bí mật cho từng loại chứng thư chữ ký số cụ thể trong Hợp đồng dịch vụ.

6.2.9 Phương pháp vô hiệu hóa khóa bí mật:

Trong trường hợp cặp khóa của HILO-CA cần phải được vô hiệu, HILO-CA sẽ thực hiện việc vô hiệu hóa một cách triệt để, đảm bảo cặp khóa sau khi bị vô hiệu hóa không thể được sử dụng bằng bất cứ hình thức nào nếu không được kích hoạt lại.

Thiết bị mật mã an toàn được vô hiệu hóa theo hướng dẫn của nhà sản xuất

6.2.10 Phương pháp hủy khóa bí mật:

Trong trường hợp cặp khóa của HILO-CA cần phải được hủy, HILO-CA sẽ thực hiện việc hủy bỏ một cách triệt để, đảm bảo cặp khóa sau khi bị hủy không thể được khôi phục hoặc sử dụng bằng bất cứ hình thức nào.

Thiết bị mật mã an toàn được hủy vật lý theo hướng dẫn của nhà sản xuất, theo chuẩn do Bộ Khoa học và Công nghệ ban hành trước khi ngừng lưu trữ.

Khóa bí mật lưu trên mô-đun mật mã được xóa bằng chứng năng xóa khóa của mô-đun mật mã.

Các hoạt động hủy bỏ khóa bí mật được ghi nhật ký.

6.2.11 Đánh giá Mô-đun mật mã:

Áp dụng chuẩn đánh giá thiết bị mật mã quy định tại phần 6.2.1.

6.3 Các vấn đề khác liên quan đến việc quản lý cặp khóa:

6.3.1 Lưu trữ khóa công khai:

Khóa công khai và chứng thư chữ ký số được lưu trữ tại kho lưu trữ của HILO-CA, theo phần 2.1.

6.3.2 Thời hạn sử dụng chứng thư chữ ký số và thời hạn sử dụng cặp khóa:

Thời gian hoạt động của chứng thư chữ ký số được bắt đầu từ thời điểm phát hành được ghi trong thuộc tính của chứng thư chữ ký số và kết thúc tại thời điểm hết hạn có đề cập trong chứng thư chữ ký số ngoại trừ trường hợp chứng thư chữ ký số bị thu hồi trước thời hạn. Thời gian hoạt động của cặp khóa bằng thời gian hoạt động của chứng thư chữ ký số tương ứng, ngoại trừ trường hợp chúng được dùng để giải mã và kiểm tra chữ ký.

Thời gian hiệu lực được quy định theo các mức thời gian theo thỏa thuận.

Thời gian hiệu lực được ghi trên chứng thư chữ ký số.

6.4 Kích hoạt dữ liệu:

6.4.1 Khởi tạo và cài đặt dữ liệu kích hoạt:

HILO-CA chọn mật khẩu đủ mạnh để bảo vệ khóa bí mật. Yêu cầu của mật khẩu đăng nhập hệ thống cần phải:

- Được một cá nhân tạo ra;
- Có ít nhất tám ký tự;

- Có ít nhất một ký tự là chữ cái và một ký tự là chữ số;
- Có ít nhất một ký tự chữ thường;
- Một ký tự bất kỳ không lặp lại từ 3 lần trở lên;
- Không trùng tên với tên của người vận hành;
- Không chứa một phần tên trong tên của người vận hành.

6.4.2 Bảo vệ dữ liệu kích hoạt:

HILO-CA khuyến cáo thuê bao tuân theo các yêu cầu trên. Ngoài ra để tăng cường an toàn, HILO-CA khuyến khích sử dụng các cơ chế đa xác thực (token và passphrase, sinh trắc và token, sinh trắc và passphrase) cho quá trình kích hoạt khóa bí mật.

6.4.3 Các khía cạnh khác của dữ liệu kích hoạt:

- Tạo dữ liệu theo nguyên tắc phần 6.4.1.
- Kích hoạt dữ liệu
- Gửi dữ liệu kích hoạt: Khi tiến hành gửi dữ liệu kích hoạt khóa bí mật cho thuê bao, Hilo-CA sử dụng các phương pháp đảm bảo không để bị mất mát, đánh cắp, sửa đổi, để lộ hoặc sử dụng trái phép khóa bí mật.
- Hủy dữ liệu kích hoạt: Khi cần thiết, dữ liệu kích hoạt khóa bí mật sẽ được HILO-CA hủy bỏ bằng các phương pháp thích hợp, đảm bảo dữ liệu không bị mất mát, đánh cắp, sửa đổi, để lộ hoặc sử dụng trái phép khóa bí mật được bảo vệ bởi dữ liệu kích hoạt đó.

6.5 Kiểm soát an ninh máy tính:

6.5.1 Các yêu cầu kỹ thuật cụ thể về an ninh máy tính:

Hệ thống mạng của HILO-CA được tách biệt khỏi các hệ thống khác, được ngắt offline và cần truy cập vật lý để vận hành và sử dụng. Các thành phần trong hệ thống mạng của HILO-CA được phân chia theo khu vực, có các thiết bị kiểm soát, phát hiện và ngăn chặn truy cập trái phép như firewall, IDS, IPS.

HILO-CA yêu cầu mật khẩu cần được thay đổi định kỳ và tuân theo tiêu chuẩn an toàn về mật khẩu, bao gồm độ dài tối thiểu, kết hợp giữa chữ cái, chữ số và ký tự đặc biệt.

Mọi truy cập vật lý trực tiếp vào hệ thống mạng của HILO-CA do người tin cậy thực hiện. Các thao tác truy cập được kiểm soát giới hạn theo nhiệm vụ, chức năng của từng vị trí.

6.5.2 Định kỳ đánh giá an ninh hệ thống máy tính:

HILO-CA tuân theo chuẩn an toàn hệ thống máy tính ISO 27001. Công việc đánh giá và kiểm tra được tiến hành theo định kỳ và đột xuất căn cứ theo tình hình thực tế.

Bộ phận quản lý hệ thống chịu trách nhiệm xử lý các báo cáo kiểm tra khảo sát và đưa ra biện pháp, kế hoạch và triển khai giải quyết các vấn đề trong báo cáo kiểm tra.

6.6 Kiểm soát vòng đời kỹ thuật:

6.6.1 Kiểm soát phát triển hệ thống:

HILO-CA có trách nhiệm xây dựng và phát triển các phần mềm quản lý cho HILO-CA và Hilo-RA.

HILO-CA cũng cung cấp cả phần mềm cho thuê bao và người nhận để thực hiện các chức năng tương tác với HILO-CA.

6.6.2 Kiểm soát quản lý an ninh:

HILO-CA có các cơ chế, chính sách để điều khiển và giám sát cấu hình hệ thống HILO-CA.

Với các phần mềm ứng dụng, HILO-CA tạo các giá trị mã hóa để đảm bảo tính toàn vẹn khi chuyển đến người dùng.

6.6.3 Kiểm soát vòng đời hệ thống:

HILO-CA không có quy định cụ thể.

6.7 Giám sát an ninh mạng hệ thống mạng:

HILO-CA đều có các biện pháp bảo mật tương ứng với các tiêu chuẩn quy định trong chính sách về bảo mật nhằm ngăn chặn các truy cập trái phép và các hoạt động tấn công khác.

HILO-CA xây dựng hệ thống giao diện quản lý và phần mềm giám sát an ninh đảm bảo được an ninh theo quy định.

6.8 Dấu thời gian:

- HILO-CA sử dụng dịch vụ cấp dấu thời gian (Timestamp Authority – TSA) hoặc nguồn thời gian hợp lệ khác được đồng bộ theo chuẩn quốc tế, nhằm đảm bảo tính chính xác và toàn vẹn của thời điểm ký số.
- Việc cấp và kiểm soát dấu thời gian tuân thủ quy định tại Điều 27 Nghị định 23/2025/NĐ-CP.

7. ĐỊNH DẠNG CHỨNG THƯ CHỮ KÝ SỐ, DANH SÁCH THU HỒI CHỨNG THƯ CHỮ KÝ SỐ (CRL), GIAO THỨC KIỂM TRA TRẠNG THÁI CHỨNG THƯ CHỮ KÝ SỐ TRỰC TUYẾN (OCSP)

7.1 Định dạng của chứng thư số:

Chứng thư chữ ký số có định dạng X.509 phiên bản 3 (1997) và RFC 5280 - Internet X.509 Public Key Infrastructure Certificate, theo Thông tư 06/2015/TT-BTTTT.

Tối thiểu thành phần chứng thư chữ ký số phải có như sau:

<i>Trường</i>	<i>Giá trị hoặc yêu cầu</i>
Serial Number	Giá trị duy nhất được gán cho mỗi tên phân biệt (DN). Giá trị này được điều khiển bởi hệ thống máy chủ của HILO-CA và được kiểm soát theo quy tắc đặt giá trị serial number do HILO-CA quy định.
Signature Algorithm	Số hiệu của thuật toán dùng để ký chứng thư chữ ký số (Xem phần 7.1.3)
Issuer DN	Xem phần 7.1.4
Valid From	Thời gian được tính theo chuẩn thời gian quốc tế UTC. Giá trị thời gian được ghi theo định dạng trong RFC 5280.
Valid To	Thời gian được tính theo chuẩn thời gian quốc tế UTC. Giá trị thời gian được ghi theo định dạng trong RFC 5280.
Subject DN	Xem phần 7.1.4
Subject Public Key	Lưu trữ theo định dạng ghi trong RFC 5280.
Signature	Chữ ký số được tạo và lưu theo định dạng trong RFC 5280.

Bảng 2 – Thành phần chứng thư số

7.1.1 Phiên bản:

Chứng thư chữ ký số của HILO-CA có thể là X.509 phiên bản 1 hoặc phiên bản 3.

Chứng thư chữ ký số của thuê bao phải là X.509 phiên bản 3.

7.1.2 Các trường mở rộng:

a. Cách sử dụng khóa (Key Usage):

Các giá trị của trường “Key Usage” trong chứng thư chữ ký số X.509 phiên bản 3 phải tuân theo quy định trong RFC 5280.

b. Phần mở rộng của chính sách chứng thư (Certificate Policies Extension)

Phần mở rộng của chính sách chứng thư không được sử dụng trong chứng thư chữ ký số của thuê bao.

c. Tên thay thế của thuê bao (Subject Alternative Names)

Trường subjectAltName trong chứng thư chữ ký số X.509 phiên bản 3 khi sử dụng phải tuân theo quy định trong RFC 5280.

d. Các ràng buộc cơ bản (Basic Constraints)

Không có quy định.

e. Cách sử dụng khóa mở rộng (Extended Key Usage)

Chứng thư chữ ký số của HILO-CA không sử dụng trường này.

Đối với chứng thư chữ ký số của thuê bao các giá trị của trường này được sử dụng theo thỏa thuận trong *Hợp đồng dịch vụ*.

f. Điểm công bố danh sách chứng thư số bị thu hồi

Trường cRLDistributionPoints của chứng thư chữ ký số X.509 phiên bản 3 có chứa địa chỉ URL để người dùng truy cập tới CRL nhằm kiểm tra trạng thái chứng thư chữ ký số.

g. Định danh khóa cho HILO-CA

Sẽ xác định sau, theo quy định của RootCA.

h. Định danh khóa cho thuê bao

Sẽ xác định sau, theo quy định của RootCA.

7.1.3 Định danh thuật toán:

Chứng thư chữ ký số của Hilo- CA sử dụng thuật toán sau đây:

+) sha256withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsads(113549) pkcs(1) pkcs-1(1) 11}

7.1.4 Định dạng tên:

Định dạng tên của chứng thư chữ ký số tuân theo quy định trong phần 3.1.1

7.1.5 Các ràng buộc, hạn chế về tên:

Không có quy định.

7.1.6 Định danh quy chế chứng thực:

Số hiệu (OID) của CPS này sẽ được đăng ký khi hệ thống của HILO-CA chính thức đi vào hoạt động.

7.1.7 Sử dụng trường mở rộng Policy Constraint:

Không có quy định.

7.1.8 Cú pháp và ngữ nghĩa trong quy chế chứng thực:

Không có quy định.

7.1.9 Xử lý ngữ nghĩa trong trường mở rộng quan trọng Certificate Policies:

Không có quy định.

7.2 Định dạng danh sách thu hồi chứng thư chữ ký số (CRL):

CRL cần chứa các giá trị sau đây:

<i>Trường</i>	<i>Giá trị hoặc yêu cầu</i>
Version	Xem phần 7.2.1
Signature Algorithm	Thuật toán dùng để ký danh sách chứng thư chữ ký số bị thu hồi.
Issuer	Thực thể thi hành ký và phát hành danh sách chứng thư chữ ký số bị thu hồi.
Effective Date	Ngày có hiệu lực của danh sách chứng thư chữ ký số bị thu hồi. Các CRL có hiệu lực ngay khi phát hành.
Next Update	Ngày cập nhật phiên bản tiếp theo của danh sách chứng thư chữ ký số bị thu hồi.
Revoked Certificates	Danh các các chứng thư chữ ký số bị thu hồi, bao gồm số hiệu (Serial Number) của chứng thư chữ ký số bị thu hồi và ngày thu hồi.

Bảng 3 – Thành phần của CRL

7.2.1 Số phiên bản của CRL:

HILO-CA hỗ trợ định dạng CRL theo phiên bản 1 hoặc phiên bản 2 của RFC 5280.

7.2.2 CRL và phần mở rộng đầu vào CRL:

Không có quy định.

7.3 Định dạng giao thức kiểm tra trạng thái chứng thư chữ ký số trực tuyến (OCSP):

Giao thức kiểm tra trạng thái chứng thư chữ ký số trực tuyến OCSP (Online Certificate Status Protocol) là giao thức cho phép kiểm tra trạng thái chứng thư chữ ký số trực tuyến.

7.3.1 Số phiên bản của OCSP:

HILO-CA hỗ trợ giao thức OCSP phiên bản 1 được khuyến nghị tuân theo chuẩn RFC 2560.

7.3.2 Phần mở rộng OCSP:

Không có quy định.

8. KIỂM ĐỊNH TÍNH TUÂN THỦ VÀ CÁC ĐÁNH GIÁ KHÁC

8.1 Tần suất và các tình huống kiểm tra kỹ thuật:

Đánh giá kiểm tra được thực hiện định kỳ hàng năm bởi đơn vị kiểm định đáp ứng yêu cầu theo quy định của pháp luật và yêu cầu của HILO-CA.

Các tình huống kiểm tra kỹ thuật theo kịch bản kiểm tra tùy theo từng thời kỳ hoạt động.

8.2 Danh tính và khả năng của đơn vị, người kiểm tra:

Đơn vị kiểm định thực hiện kiểm tra HILO-CA phải là đơn vị độc lập có khả năng sau:

- Có năng lực thành thạo về công nghệ hạ tầng khóa công khai, công cụ và kỹ thuật an toàn thông tin.
- Được chứng nhận bởi RootCA.

Danh tính và khả năng của đơn vị, người kiểm tra được HILO-CA công bố trong phần công bố kết quả kiểm tra kỹ thuật.

8.3 Tính độc lập của bên đánh giá đối với tổ chức được đánh giá:

Phạm vi đánh giá bao gồm môi trường hoạt động của HILO-CA, các hoạt động quản lý khóa, các quy trình kiểm soát điều khiển và quản trị HILO-CA, quản lý thời gian sống của các chứng thư chữ ký số và quá trình thực tế hoạt động kinh doanh.

Các nội dung kiểm tra kỹ thuật, bảo trì hệ thống bao gồm:

- Hạ tầng hệ thống.
- Các quy trình quản lý khóa.
- Quy trình vận hành hệ thống.
- Các nội dung khác theo yêu cầu của đơn vị kiểm tra kỹ thuật.

8.4 Xử lý khi phát hiện sai sót:

Căn cứ theo kết quả đánh giá và kiểm định, các vấn đề sự cố và thiếu sót phải được chỉ ra và xử lý bởi bộ phận quản lý của HILO-CA.

Nếu vấn đề là do thiết bị không đảm bảo: Lên phương án thay thế ngay thiết bị đáp ứng yêu cầu vận hành hệ thống.

Nếu sai sót ở quy trình quản lý khóa: Rà soát lại toàn bộ quy trình phân công và thực hiện quản lý khóa, ngay lập tức đưa quy trình về hoạt động đúng như CPS quy định.

Nếu sai sót ở quy trình vận hành: Tiến hành rà soát, tư vấn, nâng cấp quy trình vận hành ngay lập tức.

Đối với các nội dung không quá nguy hiểm cho hệ thống: Rà soát và khắc phục ngay khi phát hiện.

HILO-CA cam kết tuân theo các quy trình đề ra để đảm bảo tính an toàn, toàn vẹn và liên tục của hệ thống. Bất kì tổ chức, cá nhân nào gây nguy hại có hệ thống HILO-CA đều phải chịu trách nhiệm trước pháp luật và HILO-CA.

8.5 Công bố kết quả kiểm tra kỹ thuật:

Kết quả kiểm định hệ thống HILO-CA được công bố trên website của HILO-CA.

8.6 Tần suất và các trường hợp đánh giá:

Hàng năm, HILO-CA sẽ lên kế hoạch về tần suất và các trường hợp đánh giá để phù hợp với tình hình hoạt động thực tế và quy định của pháp luật.

9. CÁC NỘI DUNG NGHIỆP VỤ VÀ PHÁP LÝ KHÁC:

9.1 Phí/Giá:

9.1.1 Phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư chữ ký số:

Phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư chữ ký số theo quy định tại Thông tư 13/2025/TT-BTC của Bộ Trưởng Bộ Tài chính 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 chữ ký

Công ty cổ phần dịch vụ T-van Hilo



số: HILO-CA thu phần phí này từ thuê bao và có trách nhiệm nộp về cơ quan quản lý có thẩm quyền theo quy định.

9.1.2 Giá:

Giá cấp, gia hạn, thu hồi chứng thư chữ ký số: Bảng giá HILO-CA sẽ công bố công khai trên website và các tài liệu kinh doanh. HILO-CA sẽ công bố và gửi email thông báo tới thuê bao hiện hữu trước tối thiểu 30 ngày khi có thay đổi bảng giá.

9.1.3 Các loại chi phí khác:

Bao gồm:

- Thuế VAT mức 10% theo quy định.
- Phí USB Token.
- Phí theo thỏa thuận với khách hàng.

9.2 Trách nhiệm tài chính:

Thuê bao có trách nhiệm nộp lệ phí khởi tạo và duy trì theo quy định của HILO-CA khi tiến hành xin cấp chứng thư chữ ký số mới, gia hạn chứng thư chữ ký số hoặc thay đổi khóa.

HILO-CA có trách nhiệm mua bảo hiểm hoặc tự chịu trách nhiệm với thuê bao trong phạm vi thỏa thuận giữa thuê bao và công ty, thực hiện đúng theo quy định pháp luật.

9.2.1 Phạm vi bảo hiểm:

Phạm vi bảo hiểm do HILO-CA mua (nếu có) nhằm đảm bảo cho thuê bao hoặc bên thứ ba được bồi thường trong trường hợp xảy ra thiệt hại do lỗi kỹ thuật từ phía HILO-CA, lỗi trong quá trình phát hành, quản lý, hoặc thu hồi chứng thư chữ ký số. Các nội dung cụ thể có thể bao gồm nhưng không giới hạn:

- Thiệt hại do chứng thư chữ ký số được cấp không đúng quy định, sai thông tin.
- Thiệt hại do việc từ chối xác minh, xác thực sai danh tính thuê bao.
- Trường hợp hệ thống kỹ thuật của HILO-CA bị xâm nhập gây mất an toàn, ảnh hưởng đến chứng thư chữ ký số đang hoạt động.

Mức bồi thường cụ thể sẽ được xác định theo hợp đồng cung cấp dịch vụ hoặc chính sách bảo hiểm của HILO-CA được ký kết với bên cung cấp bảo hiểm.

9.2.2 Các tài sản khác:

Các tài sản liên quan đến thiết bị ký số (USB Token, HSM, phần mềm ký, thiết bị bảo mật...) không thuộc phạm vi bảo hiểm của HILO-CA, trừ khi có thỏa thuận riêng trong hợp đồng. Việc mất mát, hư hỏng hoặc sử dụng sai mục đích của các thiết bị này là trách nhiệm của thuê bao.

9.2.3 Phạm vi bảo hiểm hoặc bảo hành cho người dùng cuối:

Người dùng cuối được bảo vệ trong phạm vi trách nhiệm đã được quy định trong chính sách cung cấp dịch vụ của HILO-CA và các điều khoản hợp đồng cụ thể. HILO-CA không chịu trách nhiệm cho các thiệt hại phát sinh do lỗi từ phía người dùng như:

- Tiết lộ khóa riêng hoặc thông tin đăng nhập cho bên thứ ba.
- Cài đặt hoặc sử dụng phần mềm trái quy định gây mất an toàn thông tin.
- Không tuân thủ hướng dẫn kỹ thuật trong quá trình sử dụng chứng thư chữ ký số.

9.3 Bảo mật các thông tin nghiệp vụ:

9.3.1 Phạm vi thông tin nghiệp vụ cần được bảo mật:

Những dữ liệu sau của thuê bao, theo phần 9.3.2 sẽ được đảm bảo tính mật và riêng tư (“thông tin mật/riêng tư”):

- Các dữ liệu ứng dụng CA, được phê chuẩn hoặc không phê chuẩn;
- Các dữ liệu ứng dụng chứng thư chữ ký số;
- Các dữ liệu chuyển đổi (dữ liệu đầy đủ và các dữ liệu kiểm toán của quá trình chuyển đổi);
- Các dữ liệu kiểm định được tạo hoặc lưu giữ bởi HILO-CA hoặc một thuê bao;
- Các báo cáo kiểm định tạo bởi HILO-CA hay thuê bao (cho việc đánh giá những báo cáo này), hoặc những kiểm định viên (nội bộ hoặc bên ngoài);
- Các dự án khôi phục do tai nạn hay khôi phục sau sự cố;
- Quản lý mức độ an ninh trong hoạt động của phần cứng, phần mềm, các quản trị viên của dịch vụ chứng thư chữ ký số và của các dịch vụ khác.
- Tài liệu hướng dẫn, chuyển giao, đào tạo liên quan đến xây dựng, vận hành hệ thống và quy trình thẩm định của HILO-CA.

9.3.2 Thông tin nằm ngoài phạm vi bảo mật:

Chứng thư chữ ký số, thu hồi chứng thư chữ ký số và các thông tin về trạng thái của chứng thư chữ ký số, nơi lưu giữ của HILO-CA cùng các thông tin chứa bên trong chứng không được coi là các thông tin mật/riêng tư. Các thông tin mật/riêng tư trong phần 9.3.1 sẽ không được coi là riêng tư hoặc không được coi là bí mật nếu pháp luật có quy định khác.

9.3.3 Trách nhiệm bảo mật thông tin nghiệp vụ:

HILO-CA đảm bảo các thông tin riêng tư không bị tiết lộ với bên thứ 3.

Các đơn vị liên quan khi sử dụng tài liệu trong danh mục bảo mật của HILO-CA cần được sự cho phép của HILO-CA và cam kết không tiết lộ cho bất kì bên nào khác.

9.4 Bảo vệ dữ liệu cá nhân:

9.4.1 Biện pháp bảo vệ dữ liệu cá nhân:

HILO-CA áp dụng các biện pháp kỹ thuật và tổ chức phù hợp để bảo vệ dữ liệu cá nhân khỏi truy cập trái phép, tiết lộ, thay đổi hoặc phá hủy.

Dữ liệu cá nhân được lưu trữ và xử lý theo nguyên tắc bảo mật, giới hạn mục đích sử dụng, tối thiểu hóa dữ liệu thu thập và đảm bảo tính toàn vẹn của thông tin.

HILO-CA cam kết không chia sẻ, tiết lộ hoặc cung cấp dữ liệu cá nhân của thuê bao cho bất kỳ bên thứ ba nào, trừ khi:

- Có sự đồng ý rõ ràng của chủ thể dữ liệu;
- Theo yêu cầu của cơ quan nhà nước có thẩm quyền;
- Được quy định cụ thể trong hợp đồng cung cấp dịch vụ.

9.4.2 Phạm vi bảo vệ dữ liệu cá nhân:

Những thông tin được coi là riêng tư và thuộc phạm vi bảo vệ bao gồm nhưng không giới hạn:

- Thông tin định danh cá nhân (họ tên, số định danh cá nhân, địa chỉ, số điện thoại, email...);
- Thông tin đăng ký chứng thư chữ ký số;
- Thông tin liên quan đến giao dịch sử dụng chứng thư chữ ký số;
- Các dữ liệu phát sinh trong quá trình sử dụng dịch vụ, nếu không công bố công khai theo chính sách của HILO-CA.

Lưu ý: Các chứng thư chữ ký số đã được phát hành và các danh sách CRL (Danh sách chứng thư bị thu hồi) là thông tin có thể được công khai nhưng vẫn được HILO-CA bảo vệ trong quá trình lưu trữ và truyền tải để đảm bảo an toàn hệ thống.

9.4.3 Những thông tin cá nhân ngoài phạm vi bảo vệ:

Các thông tin sau đây không được coi là thông tin riêng tư và không thuộc phạm vi bảo vệ dữ liệu cá nhân:

- Các thông tin đã được công khai theo quy định của pháp luật hoặc chính sách công bố của HILO-CA;
- Thông tin chứa trong chứng thư chữ ký số đã phát hành, bao gồm: tên tổ chức/cá nhân, khóa công khai, thời hạn hiệu lực của chứng thư, số sê-ri chứng thư, tên đơn vị cấp phát chứng thư (CA) và các thông tin khác bắt buộc theo tiêu chuẩn chứng thư chữ ký số;
- Các thông tin đã được ẩn danh hóa, không còn khả năng xác định danh tính người dùng.

9.4.4 Trách nhiệm bảo vệ dữ liệu cá nhân:

HILO-CA cam kết sẽ thực hiện các biện pháp bảo vệ dữ liệu cá nhân của thuê bao phát sinh trong quá trình sử dụng dịch vụ của HILO-CA phù hợp và tuân thủ các quy định của pháp luật về bảo vệ dữ liệu cá nhân có hiệu lực tại từng thời điểm.

9.4.5 Thông báo và cho phép sử dụng dữ liệu cá nhân:

Theo quy định của pháp luật hoặc theo thỏa thuận giữa các bên, các thông tin riêng tư sẽ không được sử dụng mà không có sự cho phép của người sở hữu chúng.

9.4.6 Cung cấp thông tin riêng tư theo yêu cầu của Cơ quan quản lý:

HILO-CA có quyền tiết lộ hoặc cung cấp các thông tin được coi là riêng tư/mật trong các trường hợp sau:

- Việc công bố thông tin là cần thiết để đáp ứng yêu cầu chính thức bằng văn bản từ các cơ quan nhà nước có thẩm quyền theo quy định của pháp luật hiện hành (bao gồm nhưng không giới hạn ở công an, tòa án, cơ quan thanh tra, cơ quan an ninh mạng...);
- Việc công bố nhằm mục đích phục vụ công tác quản trị, thanh tra, kiểm tra, điều tra hoặc các thủ tục tố tụng do cơ quan có thẩm quyền thực hiện;

- Việc công bố được yêu cầu để đảm bảo tuân thủ các quy định pháp luật liên quan đến an toàn thông tin, bảo vệ dữ liệu cá nhân, hoặc các quy định chuyên ngành về dịch vụ chứng thực chữ ký số;

- Trong mọi trường hợp, HILO-CA chỉ cung cấp thông tin trong phạm vi cần thiết và đúng đối tượng, đồng thời ghi nhận, lưu vết toàn bộ quá trình xử lý yêu cầu theo chính sách nội bộ và quy định pháp luật.

9.4.7 Các tình huống cung cấp thông tin khác:

Ngoài các trường hợp nêu tại mục 9.4.6, HILO-CA có thể xem xét cung cấp thông tin cá nhân trong các tình huống sau, với điều kiện có sự đồng ý rõ ràng, cụ thể từ chủ thể dữ liệu:

- Khi thuê bao hoặc người dùng cuối có yêu cầu bằng văn bản hoặc thông qua kênh xác thực chính thức (giao diện quản lý tài khoản, hồ sơ dịch vụ, email xác minh...);

- Trong trường hợp phục vụ điều tra nội bộ về sự cố an toàn thông tin, hành vi vi phạm điều khoản dịch vụ hoặc gian lận, với sự chấp thuận của người có thẩm quyền trong HILO-CA và chủ thể dữ liệu;

- Khi chia sẻ thông tin với các đối tác cung cấp dịch vụ phụ trợ (subcontractors) có ký kết thỏa thuận bảo mật dữ liệu (NDA) để thực hiện một phần nghĩa vụ kỹ thuật theo hợp đồng, và trong phạm vi tối thiểu cần thiết.

9.5 Quyền sở hữu trí tuệ:

Cần xác định rõ quyền sở hữu trí tuệ giữa các thành phần tham gia dịch vụ HILO-CA

9.5.1 Quyền sở hữu trong chứng thư số và thông tin thu hồi chứng thư chữ ký số:

HILO-CA có tất cả quyền sở hữu trí tuệ liên quan đến chứng thư chữ ký số và các thông tin thu hồi chứng thư chữ ký số do HILO-CA ban hành.

HILO-CA được phép sao chép và phân phối chứng thư chữ ký số mà không cần trả phí với điều kiện phải đảm bảo tính nguyên vẹn của chứng thư chữ ký số;

HILO-CA và thuê bao cho phép người nhận sử dụng các thông tin về tình trạng thu hồi của chứng thư chữ ký số để thực hiện chức năng của mình tuân theo thỏa thuận sử dụng CRL, thỏa thuận với người nhận hay các thỏa thuận thích hợp khác.

9.5.2 Quyền sở hữu trong CPS:

Các thành phần tham gia dịch vụ HILO-CA chấp nhận rằng HILO-CA có quyền sở hữu trí tuệ đối với CPS và các điều khoản ghi trong CPS này.

9.5.3 Quyền sở hữu tên:

Người đăng ký chứng thư chữ ký số có quyền sở hữu đối với thương hiệu, tên dịch vụ trong các ứng dụng chứng thư chữ ký số, và với tên phân biệt (distinguished name) trong chứng thư chữ ký số cấp.

9.5.4 Quyền sở hữu khóa và các tài liệu của khóa:

Cặp khóa tương ứng với chứng thư chữ ký số của HILO-CA và thuê bao là tài sản của HILO-CA và thuê bao, được lưu trữ và bảo vệ theo quy định của pháp luật về quyền sở hữu trí tuệ.

9.6 Tuyên bố và cam kết:

9.6.1 Tuyên bố và cam kết của tổ chức phát hành chứng thư chữ ký số:

Các dịch vụ HILO-CA bảo đảm:

- Không có những thông tin sai lệch với thực tế trong chứng thư chữ ký số;
 - Không có sai sót ở các thông tin trong chứng thư chữ ký số;
 - Chứng thư chữ ký số của HILO-CA phù hợp với yêu cầu trong CPS;
 - Dịch vụ thu hồi chứng thư chữ ký số và sử dụng kho lưu trữ phù hợp với tiêu chuẩn trong CPS.
- HILO-CA xác nhận trong quá trình cung cấp dịch vụ chứng thực chữ ký số cho khách hàng, HILO-CA thực hiện các hoạt động xử lý dữ liệu cá nhân để cung cấp dịch vụ cho khách hàng theo quy định tại Nghị định 23/2025/NĐ-CP ngày 21/02/2025 của Chính phủ quy định về chữ ký điện tử và dịch vụ tin cậy và Nghị định 13/2023/NĐ-CP ngày 7/04/2023 của Chính phủ về bảo vệ dữ liệu cá nhân.

Thỏa thuận với thuê bao có thể có thêm các tuyên bố và cam kết khác.

9.6.2 Tuyên bố và cam kết của Thuê bao:

Thuê bao cam kết rằng:

- Mỗi chữ ký số được tạo sử dụng khóa bí mật tương ứng với khóa công khai liệt kê trong chứng thư chữ ký số là chữ ký số của thuê bao. Chứng thư chữ ký số được

chấp nhận và hoạt động (khi chưa hết hạn hay bị thu hồi) trong thời gian chữ ký điện tử này được tạo.

- Khóa bí mật được bảo vệ và người không có thẩm quyền không thể truy cập vào khóa này.

- Tất cả các cam kết được đưa ra bởi thuê bao trong ứng dụng chứng thư chữ ký số là

- đúng sự thật.

- Tất cả những thông tin cung cấp bởi thuê bao và chứa bên trong chứng thư chữ ký số là đúng sự thật.

- Chứng thư chữ ký số được sử dụng cho các mục đích hợp pháp và tuân theo những yêu cầu trong CPS này.

- Thuê bao là người dùng cuối và không phải là một CA, không được phép sử dụng khóa bí mật kết hợp với bất kì khóa công khai nào được liệt kê trong chứng thư chữ ký số cho các mục đích ký số, hay đưa ra CRL, như là một CA.

Hợp đồng dịch vụ giữa HILO-CA với thuê bao có thể có thêm các thỏa thuận và cam kết khác.

9.6.3 Tuyên bố và cam kết của bên tin tưởng:

Các HILO-RA bảo đảm:

- Không có những thông tin sai lệch với thực tế trong chứng thư chữ ký số;
- Không có sai sót ở các thông tin trong chứng thư chữ ký số;
- Những chứng thư chữ ký số của Hilo-RA cung cấp tuân theo các yêu cầu trong CPS này;
- Dịch vụ thu hồi chứng thư chữ ký số và sử dụng kho lưu trữ phù hợp với tiêu chuẩn trong CPS này.

Thỏa thuận với thuê bao có thể có thêm các tuyên bố và cam kết khác.

9.6.4 Tuyên bố và cam kết của các bên liên quan khác:

Không có qui định.

9.7 Từ chối bảo lãnh:

Trong giới hạn cho phép của luật pháp, hợp đồng thuê bao và người nhận có thể bị HILO-CA từ chối bảo lãnh nếu lỗi không phải do HILO-CA gây ra.

9.8 Giới hạn 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 HILO-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 HILO-CA sẽ được thiết lập trong *Hợp đồng dịch vụ*.

9.9 Bồi thường thiệt hại:

HILO-CA chịu trách nhiệm bồi thường cho Thuê bao và người nhận trong trường hợp phát sinh lỗi từ hệ thống gây ảnh hưởng nghiêm trọng tới Thuê bao.

9.9.1 Vấn đề bồi thường của thuê bao:

Thuê bao phải bồi thường cho HILO-CA nếu xuất hiện:

- Những thông tin sai lệch hoặc xuyên tạc sự thật do thuê bao cung cấp trên dịch vụ chứng thư chữ ký số;
- Lỗi của thuê bao để lộ những nhân tố, yếu tố liên quan đến dịch vụ chứng thư chữ ký 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.

9.9.2 Vấn đề bồi thường của người nhận:

Khi được pháp luật cho phép, HILO-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 chữ ký số không được đáp ứng trong một số trường hợp;

- Lỗi của người nhận trong việc kiểm tra trạng thái của chứng thư chữ ký số để xác định chứng thư chữ ký số đã hết hạn hay bị thu hồi.

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

9.10 Hiệu lực của CPS:

9.10.1 Thời hạn của CPS:

CPS này bắt đầu có hiệu lực khi hệ thống HILO-CA chính thức đi vào hoạt động.

Các điều sửa đổi bổ sung cho CPS này cần được sự đồng ý của ROOT-CA và có hiệu lực khi có sự công bố từ kho lưu trữ của dịch vụ HILO-CA.

CPS này này khi được bổ sung, sửa đổi sẽ vẫn giữ hiệu lực cho đến khi được thay thế bởi một văn bản mới.

9.10.2 Chấm dứt hiệu lực và các tồn tại:

- Khi CPS này hết hiệu lực (do được thay thế hoặc dừng cung cấp dịch vụ), điều đó không làm ảnh hưởng đến hiệu lực của các chứng thư số đã được ban hành trước đó, trừ khi có thông báo thu hồi hoặc chấm dứt rõ ràng.

- Các điều khoản còn hiệu lực liên quan đến nghĩa vụ bảo mật, lưu trữ dữ liệu, trách nhiệm pháp lý, bảo vệ người dùng và xử lý tranh chấp vẫn tiếp tục được áp dụng cho đến khi hoàn thành đầy đủ các nghĩa vụ liên quan.

- Việc chấm dứt CPS sẽ không giải phóng HILO-CA khỏi trách nhiệm đối với các nghĩa vụ đã phát sinh trong thời gian CPS còn hiệu lực.

9.10.3 Ảnh hưởng của việc chấm dứt hiệu lực:

Việc CPS hết hiệu lực có thể dẫn đến các thay đổi trong chính sách cung cấp dịch vụ, quy trình quản lý chứng thư, hoặc cơ cấu vận hành của HILO-CA.

Người dùng, thuê bao và các bên liên quan sẽ được thông báo tối thiểu **30 ngày** trước khi CPS bị chấm dứt hoặc thay thế (trừ trường hợp khẩn cấp do yêu cầu của cơ quan quản lý nhà nước).

Các chứng thư số đang còn hiệu lực tại thời điểm CPS bị chấm dứt sẽ:

- Tiếp tục có hiệu lực theo thời hạn đã được quy định trong chứng thư;
- Hoặc bị xem xét thu hồi nếu có yêu cầu từ cơ quan quản lý hoặc phát hiện rủi ro an toàn thông tin nghiêm trọng liên quan đến nội dung thay thế của CPS mới.

Các bên sử dụng dịch vụ có trách nhiệm xem xét và cập nhật tuân thủ theo CPS mới khi có thay đổi, và HILO-CA sẽ đảm bảo cung cấp thông tin đầy đủ, minh bạch trong quá trình chuyển đổi.

9.11 Thông báo và trao đổi thông tin với các bên tham gia:

HILO-CA sẽ sử dụng các biện pháp thích hợp để thông báo cho các bên liên quan về nội dung sửa đổi, bổ sung CPS này.

Các phiên bản của CPS được HILO-CA lưu và công bố đầy đủ trên website của mình tại link: <https://HILO-CA.vn/tai-lieu>

9.12 Bổ sung và sửa đổi:

9.12.1 Quy trình sửa đổi:

Những sửa đổi của CPS này sẽ được thực hiện bởi HILO-CA. Những điều sửa đổi có thể ở dạng tài liệu chứa tất cả những điều sửa đổi cho CPS hoặc ở dạng cập nhật. Phiên bản sửa đổi hay cập nhật được liên kết đến phần thông báo và cập nhật trong kho lưu trữ của dịch vụ HILO-CA tại địa chỉ <https://HILO-CA.vn/tai-lieu/>

HILO-CA có quyền quyết định việc thay đổi là cần thiết hay không cần thiết.

Những đề xuất thay đổi CPS sẽ được nêu ra trong tài liệu của HILO-CA tại địa chỉ: <https://HILO-CA.vn/tai-lieu/> sau khi được Bộ Khoa học và công nghệ chấp nhận.

HILO-CA tập hợp những đề nghị thay đổi CPS từ các thành phần tham gia dịch vụ HILO-CA. Nếu HILO-CA cho rằng một sự thay đổi nào đó là cần thiết thì việc thay đổi sẽ được thực hiện.

Ngoài ra, nếu HILO-CA cho rằng thay đổi CPS là cần thiết để ngăn chặn xâm phạm đến an toàn của dịch vụ HILO-CA, thì việc thay đổi sẽ ngay lập tức được thực hiện và có hiệu lực.

9.12.2 Cơ chế và thời hạn thông báo:

Thời điểm có hiệu lực của việc sửa đổi là 15 ngày kể từ ngày được công bố trên kho lưu trữ của dịch vụ HILO-CA. Bất kỳ ai tham gia vào dịch vụ HILO-CA cũng có quyền đề xuất ý kiến tới HILO-CA cho đến lúc hết thời gian sửa đổi.

9.12.3 Các trường hợp cần thay đổi OID (Object identifier-mã định danh đối tượng):

HILO-CA sẽ xem xét tất cả các đề xuất liên quan đến vấn đề sửa đổi bổ sung và có thể:

- Cho phép các đề xuất có hiệu lực mà không cần sửa đổi;
- Sửa đổi các đề xuất và tái bản nếu cần;
- Hủy bỏ những đề xuất sửa đổi.

HILO-CA có quyền hủy bỏ các đề xuất sửa đổi, và đưa ra ghi chú trong tài liệu của HILO-CA. Những sửa đổi có hiệu lực sau khi hết hạn sửa đổi.

Nếu cần thiết, HILO-CA có thể thay đổi OID cho các chính sách chứng thư chữ ký số tương ứng với từng cấp chứng thư chữ ký số. Nếu không, việc sửa đổi sẽ không bao gồm việc sửa đổi OID.

9.13 Thủ tục giải quyết khiếu nại:

9.13.1 Tranh chấp giữa HILO-CA, đối tác và thuê bao:

Việc giải quyết tranh chấp giữa HILO-CA, người nhận và thuê bao phải tuân thủ theo các điều khoản được ghi trong hợp đồng và trên cơ sở quy định của pháp luật.

9.13.2 Tranh chấp với thuê bao hay người nhận:

Trường hợp này được thực hiện theo quy định của pháp luật.

9.14 Hệ thống căn cứ pháp lý:

Tài liệu Quy chế chứng thực của các tổ chức cung cấp dịch vụ chứng thực chữ ký số được điều chỉnh bởi các văn bản quy phạm pháp luật, bao gồm:

- Luật giao dịch điện tử: Luật số 20/2023/QH15 ngày 22/06/2023.
- Nghị định số 23/2025/NĐ-CP ngày 21/2/2025 của Chính phủ quy định về chữ ký điện tử và dịch vụ tin cậy;
- Thông tư 13/2025/TT-BTC ngày 19/03/2025 quy định về mức thu, chế độ thu, nộp, quản lý và sử dụng phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư chữ ký số.

CPS này được xây dựng theo quy định của pháp luật của nước Cộng hòa xã hội chủ nghĩa Việt Nam.

9.15 *Tuân thủ quy định pháp luật hiện hành:*

Trong trường hợp điều ước quốc tế mà Việt Nam tham gia hoặc phê chuẩn có quy định khác pháp luật trong nước thì áp điều ước đó.

- Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;
- Luật An ninh mạng ngày 12 tháng 06 năm 2018;
- Luật Dữ liệu ngày 30 tháng 11 năm 2024;
- Nghị định số 13/2023/NĐ-CP ngày 25 tháng 06 năm 2023 của Chính phủ về bảo vệ dữ liệu cá nhân;
- Nghị định số 69/2024/NĐ-CP ngày 25 tháng 06 năm 2024 của Chính phủ quy định về định danh và xác thực điện tử;
- ...

Các tổ chức, cá nhân có trách nhiệm cung cấp thông tin phục vụ công tác đấu tranh, phòng, chống tội phạm lợi dụng dịch vụ để thực hiện các hành vi vi phạm pháp luật.

9.16 *Các điều khoản chung:*

9.16.1 *Thỏa thuận toàn bộ:*

Không có quy định.

9.16.2 *Chuyển nhượng:*

Không có quy định.

9.16.3 *Tính độc lập của các điều khoản:*

Trong trường hợp một điều khoản hay sự sửa đổi bổ sung của CPS được giữ lại không thể thi hành được bởi quy định của pháp luật hoặc quyết định của cơ quan nhà nước có thẩm quyền thì phần còn lại của Quy chế vẫn có hiệu lực.

9.16.4 *Sự thực thi (quyền ủy nhiệm và quyền khước từ):*

Bất kỳ một bên nào chiếm ưu thế trong những tranh cãi nảy sinh ngoài hợp đồng đều được quyền ủy nhiệm hoặc quyền khước từ do sự vi phạm một trong các điều khoản trong hợp đồng.

9.16.5 *Sự kiện bất khả kháng:*

Trong phạm vi luật pháp cho phép, thỏa thuận của thuê bao và thỏa thuận bên liên quan bắt buộc phải tuân theo các điều khoản bảo vệ dịch vụ HILO-CA.

Công ty cổ phần dịch vụ T-van Hilo



9.17 Các điều khoản khác:

Không có quy định.

PHỤ LỤC

Danh mục định nghĩa và thuật ngữ viết tắt

Thuật ngữ	Giải thích
<i>24 x 7</i>	24 giờ/ngày và 7 ngày/tuần
<i>Bộ Thông tin và Truyền thông (Nay là Bộ Khoa học và Công nghệ)</i>	Bộ Khoa học và Công nghệ là cơ quan của Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam
<i>CA</i>	Certificate Authority – Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng.
<i>Chữ ký số</i>	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.
<i>Chứng thư chữ ký số</i>	là một dạng chứng thư chữ ký số điện tử do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp cho thuê bao.
<i>Chứng thư số có hiệu lực</i>	là chứng thư chữ ký số chưa hết hạn, không bị tạm dừng hoặc bị thu hồi.
<i>CP</i>	Certificate Policies – Chính sách chứng thư.
<i>CPS</i>	Certification Practice Statement – Quy chế chứng thực.
<i>CRL</i>	Certificate Revocation List – Danh sách chứng thư chữ ký số bị thu hồi.

<i>Dịch vụ chứng thực chữ ký số</i>	là 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, tạm dừng, phục hồi 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.
<i>Hệ thống mật mã không đối xứng</i>	là hệ thống mật mã có khả năng tạo được cặp khóa bao gồm khóa bí mật và khóa công khai.
<i>Hợp đồng dịch vụ</i>	Hợp đồng cung cấp và sử dụng dịch vụ chứng thực chữ ký số công cộng giữa HILO-CA – CA và người sử dụng dịch vụ.
<i>Khoá</i>	là một chuỗi các số nhị phân (0 và 1) dùng trong các hệ thống mật mã.
<i>Khóa bí mật</i>	là một khóa trong cặp khóa thuộc hệ thống mật mã không đối xứng, được dùng để tạo chữ ký số.
<i>Khóa công khai</i>	là 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 khóa bí mật tương ứng trong cặp khóa.
<i>Ký số</i>	là 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.
<i>Người ký</i>	là thuê bao dùng đúng khóa bí mật của mình để ký số vào một thông điệp dữ liệu dưới tên của mình.
<i>Người nhận</i>	là tổ chức, cá nhân nhận được thông điệp dữ liệu được ký số bởi người ký, sử dụng chứng thư chữ ký 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.

<i>OCSP</i>	Online Certificate Status Protocol - là giao thức cho phép kiểm tra trạng thái chứng thư chữ ký số trực tuyến.
<i>CRL</i>	Certificate Revoke List – Là danh sách chứng thư chữ ký số bị thu hồi
<i>PKI</i>	Public Key Infrastructure – Hạ tầng khóa công khai.
<i>RA</i>	Registration Authority – Tổ chức tiếp nhận đăng ký và xác thực thông tin của người sử dụng dịch vụ.
<i>Tạm dừng chứng thư số</i>	là làm mất hiệu lực của chứng thư chữ ký số một cách tạm thời từ một thời điểm xác định.
<i>Thu hồi chứng thư số</i>	là làm mất hiệu lực của chứng thư chữ ký số một cách vĩnh viễn từ một thời điểm xác định.
<i>Thuê bao</i>	là tổ chức, cá nhân được cấp chứng thư chữ ký số, chấp nhận chứng thư số và giữ khoá bí mật tương ứng với khoá công khai ghi trên chứng thư chữ ký số được cấp đó.
<i>Tổ chức cung cấp dịch vụ chứng thực chữ ký số</i>	là 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.
<i>Hilo</i>	Công ty Cổ phần Dịch vụ T-Van Hilo
<i>HILO-CA</i>	Dịch vụ chứng thực chữ ký số công cộng do Công ty cổ phần Dịch vụ T-Van Hilo cung cấp/và Công ty cổ phần Dịch vụ T-Van (Hilo) với tư cách là nhà cung cấp dịch vụ chứng thực chữ ký số công cộng.
<i>Hilo-RA</i>	Tổ chức tiếp nhận yêu cầu cung cấp dịch vụ và xác thực thông tin thuê bao HILO-CA ủy quyền.
<i>Xác thực định danh</i>	là hoạt động nhằm chứng minh thông tin định danh của thuê bao, người yêu cầu cấp chứng thư chữ ký số.