BỘ QUỐC PHÒNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 1546/QĐ-BQP

Hà Nội, ngày 31 tháng 3 năm 2026

QUYẾT ĐỊNH
Ban hành Khung kiến trúc hạ tầng mật mã quốc gia

BỘ TRƯỞNG BỘ QUỐC PHÒNG

Căn cứ Luật Cơ yếu số 05/2011/QH13;

Căn cứ Luật An ninh mạng số 116/2025/QH15;

Căn cứ Luật Bảo vệ bí mật nhà nước số 117/2025/QH15;

Căn cứ Nghị định số 01/2022/NĐ-CP ngày 30 tháng 11 năm 2022 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Quốc phòng; Nghị định số 03/2025/NĐ-CP ngày 28 tháng 02 năm 2025 của Chính phủ sửa đổi, bổ sung một số điều của Nghị định số 01/2022/NĐ-CP ngày 30 tháng 11 năm 2022 của Chính phủ;

Căn cứ Nghị định số 09/2014/NĐ-CP ngày 27 tháng 01 năm 2014 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Ban Cơ yếu Chính phủ;

Căn cứ Nghị quyết số 57-NQ/TW ngày 22 tháng 12 năm 2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia;

Căn cứ Quy định số 05-QĐ/BCĐTW ngày 27 tháng 8 năm 2025 của Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia ban hành Quy định về mô hình liên thông số thống nhất, hiệu quả và quản trị dựa trên dữ liệu trong hệ thống chính trị;

Căn cứ Kế hoạch số 04-KH/BCĐTW ngày 05 tháng 01 năm 2026 của Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị;

Theo đề nghị của Trưởng ban Ban Cơ yếu Chính phủ tại Tờ trình số 141/TTr-BCY ngày 09 tháng 3 năm 2026.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Khung kiến trúc hạ tầng mật mã quốc gia.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 3. Trưởng ban Ban Cơ yếu Chính phủ, Thủ trưởng các cơ quan, đơn vị và các cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Ban Chỉ đạo TW về phát triển KHCN, ĐMST&CĐS (để b/c);
- Thủ tướng và các Phó Thủ tướng Chính phủ (để b/c);
- Văn phòng Trung ương Đảng và các Ban Đảng TW;
- Các Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- Văn phòng Quốc hội;
- Văn phòng Chủ tịch nước;
- Văn phòng Ủy ban Trung ương Mặt trận Tổ quốc VN;
- Tòa án nhân dân tối cao;
- Viện kiểm sát nhân dân tối cao;
- Kiểm toán Nhà nước;
- Tỉnh ủy/Thành ủy, UBND các tỉnh, thành phố;
- Các cơ quan, đơn vị thuộc Bộ Quốc phòng;
- Ban Cơ yếu Chính phủ;
- Cổng Thông tin điện tử Bộ Quốc phòng;
- Lưu: VT, CCHC. Ph127.

BỘ TRƯỞNG

BỘ QUỐC PHÒNG

Đại tướng Phan Văn Giang

BỘ QUỐC PHÒNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

KHUNG KIẾN TRÚC HẠ TẦNG MẬT MÃ QUỐC GIA

(Kèm theo Quyết định số 1546/QĐ-BQP ngày 31/3/2026 của Bộ trưởng Bộ Quốc phòng)

I. MÔ HÌNH KHUNG KIẾN TRÚC HẠ TẦNG MẬT MÃ QUỐC GIA

1. Giới thiệu chung

Mô hình Khung kiến trúc hạ tầng mật mã quốc gia được xây dựng nhằm thiết lập một nền tảng chuẩn hóa, đồng bộ, thống nhất việc ứng dụng, triển khai và quản lý các giải pháp mật mã trong toàn bộ hệ thống chính trị; đóng vai trò quan trọng trong việc tăng cường năng lực bảo vệ an ninh mạng, bảo vệ chủ quyền số quốc gia và bảo đảm hoạt động thông suốt, tin cậy của các hệ thống thông tin thuộc toàn bộ hệ thống chính trị. Khung kiến trúc này quy định các nguyên tắc, cấu phần chức năng, yêu cầu kỹ thuật và phương thức kết nối giữa các thành phần mật mã, tạo cơ sở để bảo đảm an toàn, bí mật và toàn vẹn cho các hoạt động xử lý, lưu trữ, trao đổi thông tin của các cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc Việt Nam, các tổ chức chính trị và tổ chức chính trị - xã hội từ Trung ương đến địa phương.

Với vai trò là định hướng tổng thể việc phát triển, vận hành các hệ thống mật mã chuyên dụng và dân sự, mô hình Khung kiến trúc giúp bảo đảm sự liên thông, tương thích và tuân thủ thống nhất các quy định của pháp luật, tiêu chuẩn, quy chuẩn kỹ thuật quốc gia về bảo vệ thông tin bí mật nhà nước, an toàn thông tin; đồng thời, tạo điều kiện thuận lợi cho việc tích hợp công nghệ tiên tiến, nâng cao năng lực bảo mật, giảm thiểu rủi ro và hỗ trợ các cơ quan, tổ chức trong xây dựng hệ sinh thái số an toàn, bền vững.

2. Phạm vi áp dụng

Mô hình Khung kiến trúc hạ tầng mật mã quốc gia được áp dụng thống nhất trong toàn bộ hệ thống chính trị, bao gồm: Các cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc Việt Nam, các tổ chức chính trị và tổ chức chính trị - xã hội từ Trung ương đến địa phương.

3. Mục tiêu, tầm nhìn

3.1. Mục tiêu đến năm 2030: Xây dựng, triển khai, vận hành đồng bộ mô hình Khung kiến trúc hạ tầng mật mã quốc gia trong toàn bộ hệ thống chính trị, bảo đảm thống nhất, liên thông và tuân thủ nghiêm ngặt các quy định của pháp luật về bảo vệ bí mật nhà nước. Tất cả các cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc Việt Nam, các tổ chức chính trị và tổ chức chính trị - xã hội từ Trung ương đến địa phương được triển khai và áp dụng hiệu quả các giải pháp mật mã bảo vệ bí mật nhà nước theo mô hình Khung kiến trúc thống nhất. Hình thành hệ thống các nền tảng, dịch vụ và giải pháp mật mã đáp ứng yêu cầu bảo mật cấp độ cao, hỗ trợ chuyển đổi số phục vụ công tác lãnh đạo, quản lý và điều hành. Xây dựng đội ngũ cán bộ chuyên trách

có năng lực, được đào tạo bài bản, đủ khả năng vận hành, kiểm soát và ứng phó hiệu quả trước các nguy cơ tấn công an ninh mạng ngày càng phức tạp.

3.2. Tầm nhìn đến 2045: Đến năm 2045, xây dựng hệ sinh thái mật mã bảo vệ thông tin bí mật nhà nước hiện đại, tự chủ, bền vững, đáp ứng yêu cầu bảo vệ an ninh quốc gia trong môi trường số hóa toàn diện. Hệ thống mật mã được phát triển theo kiến trúc mở, linh hoạt, thích ứng nhanh với sự thay đổi của công nghệ và các hình thức tấn công mạng mới. Các cơ quan, tổ chức trong toàn bộ hệ thống chính trị vận hành thống nhất một nền tảng bảo mật tiên tiến, tích hợp sâu với hạ tầng số quốc gia, bảo đảm bí mật, an toàn, tin cậy tuyệt đối cho mọi hoạt động xử lý và trao đổi thông tin bí mật nhà nước. Việt Nam trở thành quốc gia có năng lực làm chủ công nghệ mật mã trọng yếu, từng bước tham gia vào chuỗi phát triển, đóng góp vào tiêu chuẩn mật mã quốc tế, khẳng định vị thế, năng lực bảo vệ chủ quyền số và an ninh thông tin quốc gia trong dài hạn.

4. Nguyên tắc xây dựng

4.1. Nguyên tắc thống nhất, đồng bộ trong toàn hệ thống chính trị: Khung kiến trúc hạ tầng mật mã quốc gia được triển khai thống nhất, đồng bộ trong toàn bộ hệ thống chính trị, bao gồm: Các cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc Việt Nam, các tổ chức chính trị và tổ chức chính trị - xã hội từ Trung ương đến địa phương.

4.2. Nguyên tắc dùng chung, liên thông: Các thành phần và dịch vụ mật mã được thiết kế, triển khai dùng chung, liên thông, ưu tiên cung cấp qua giao diện lập trình ứng dụng (API); bảo đảm tiết kiệm, hiệu quả, quản lý thống nhất, không trùng lặp về đầu tư, hạ tầng và nền tảng. Đây là cơ chế kỹ thuật để hiện thực hóa "hệ sinh thái dịch vụ hợp nhất", lấy người dùng làm trung tâm.

4.3. Nguyên tắc bảo đảm an ninh mạng và chủ quyền số quốc gia: Khung kiến trúc hạ tầng mật mã quốc gia là một bộ phận cốt lõi trong bảo đảm an ninh mạng và chủ quyền số quốc gia. Tất cả dữ liệu, giao dịch, danh tính số trong toàn bộ hệ thống chính trị phải được bảo vệ bằng các thuật toán, thiết bị và tiêu chuẩn mật mã do Việt Nam làm chủ. Ưu tiên phát triển, ứng dụng các công nghệ mật mã tiên tiến, mật mã hậu lượng tử và giải pháp tự chủ về an toàn thông tin.

4.4. Nguyên tắc mở, linh hoạt và khả năng tích hợp cao: Khung kiến trúc hạ tầng mật mã quốc gia được xây dựng theo mô hình kiến trúc mở, có khả năng tích hợp, mở rộng linh hoạt, đáp ứng sự thay đổi nhanh của công nghệ và yêu cầu thực tiễn. Các hệ thống và thành phần mật mã phải bảo đảm kết nối, tương thích với các nền tảng số quốc gia, dữ liệu mở và hệ thống của các bộ, ngành, địa phương.

4.5. Nguyên tắc dữ liệu là trung tâm, bảo mật theo vòng đời dữ liệu: Dữ liệu là tài nguyên cốt lõi cần được bảo vệ xuyên suốt toàn bộ vòng đời, bao gồm thu thập, xử lý, lưu trữ, chia sẻ và hủy bỏ. Toàn bộ hệ thống thông tin trong phạm vi áp dụng của Khung kiến trúc hạ tầng mật mã quốc gia phải triển khai cơ chế mã hóa, ký số, xác thực và kiểm soát truy cập tương ứng với mức độ phân loại dữ liệu, bảo đảm nguyên tắc "dữ liệu nhập một lần - được sử dụng, bảo vệ nhiều lần". Đây là cơ sở kỹ thuật bắt buộc để bảo đảm dữ liệu "tin cậy", "chính xác" phục vụ "lãnh đạo, chỉ đạo, điều hành dựa trên dữ liệu"; đồng thời bảo đảm việc sử dụng sản phẩm, dịch vụ mật mã không cản trở vận hành hệ thống.

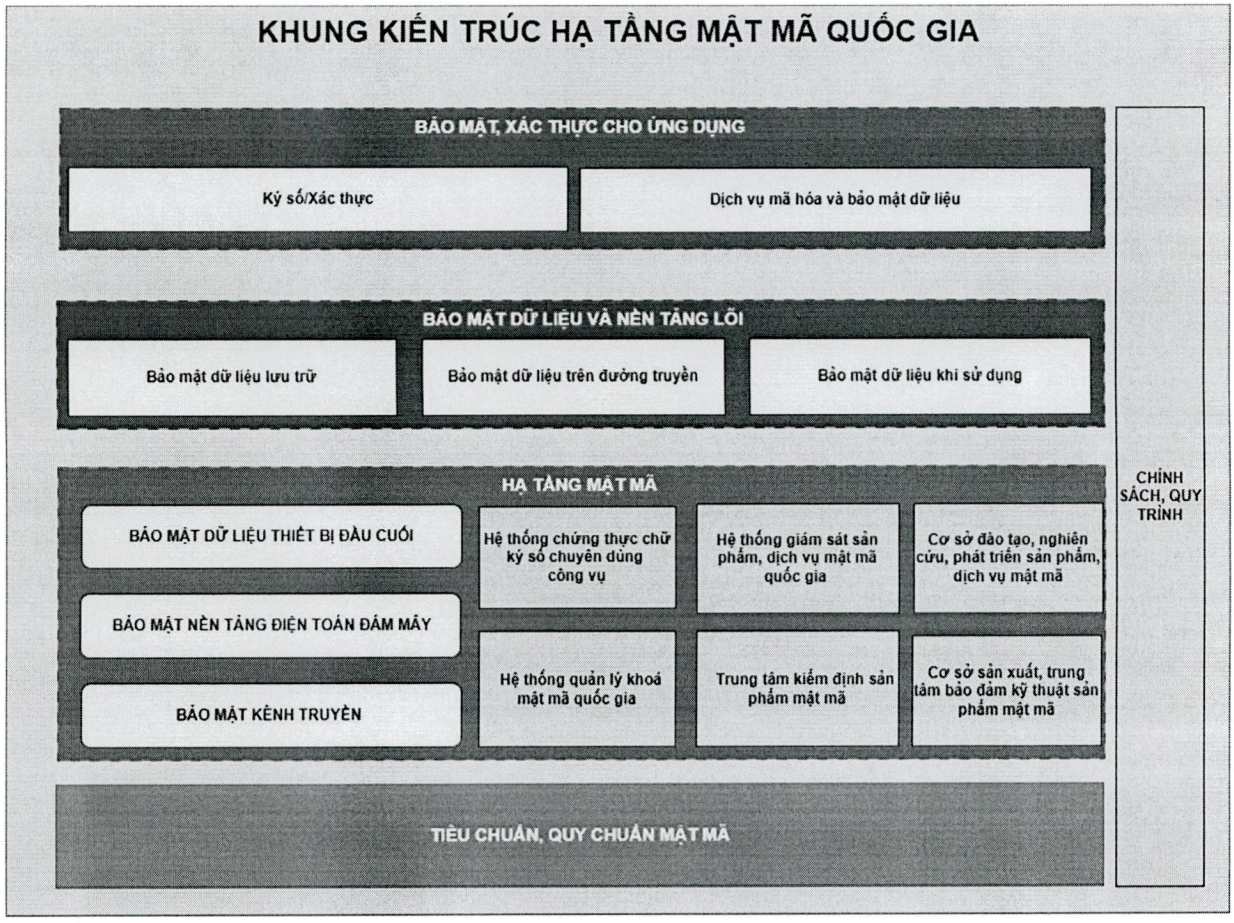
4.6. Nguyên tắc chuẩn hóa, tuân thủ và kiểm định kỹ thuật: Mọi thành phần, thiết bị, phần mềm và dịch vụ mật mã triển khai trong hệ thống chính trị phải tuân thủ các Tiêu chuẩn quốc gia (TCVN) và Quy chuẩn kỹ thuật quốc gia (QCVN) trong hoạt động mật mã để bảo vệ thông tin bí mật nhà nước. 100% sản phẩm mật mã (gồm sản phẩm thương mại và sản phẩm tự phát triển) bắt buộc phải được kiểm định, chứng nhận tại Trung tâm kiểm định sản phẩm mật mã quốc gia trước khi đưa vào sử dụng.

4.7. Nguyên tắc quản trị tập trung, vận hành phân tán: Mô hình này cho phép hiện thực hóa "Phân cấp, phân quyền mạnh mẽ trên nền tảng số".

4.7.1. Quản trị tập trung: Ban Cơ yếu Chính phủ thực hiện quản trị tập trung, thống nhất về chính sách, chiến lược, tiêu chuẩn kỹ thuật và vận hành các hạ tầng mật mã lõi dùng chung (hạ tầng khóa công khai (PKI), hệ thống quản lý khóa mật mã quốc gia, hệ thống giám sát dịch vụ, sản phẩm mật mã quốc gia).

4.7.2. Vận hành phân tán: Các ban, bộ, ngành, địa phương tự vận hành các hệ thống nghiệp vụ của mình. Đối với dữ liệu mật phải tích hợp và tuân thủ các dịch vụ mật mã dùng chung do Ban Cơ yếu Chính phủ cung cấp. Hệ thống mật mã được quản trị tập trung, thống nhất bởi Ban Cơ yếu Chính phủ nhưng triển khai vận hành phân tán tại các ban, bộ, ngành, địa phương.

5. Mô hình khái quát



Hình 1. Mô hình khái quát các thành phần trong Khung kiến trúc hạ tầng mật mã quốc gia

5.1. Tiêu chuẩn, quy chuẩn kỹ thuật mật mã: Hệ thống tiêu chuẩn, quy chuẩn đối với giao thức, thuật toán, sản phẩm mật mã, khóa mã và các thành phần liên quan là nền tảng bảo đảm sự thống nhất, đồng bộ, an toàn trong triển khai các giải pháp mật mã để bảo vệ thông tin bí mật nhà nước trong toàn bộ hệ thống chính trị.

Các tiêu chuẩn, quy chuẩn này quy định yêu cầu kỹ thuật tối thiểu đối với thuật toán mật mã sử dụng cho mã hóa, giải mã, xác thực, ký số và bảo đảm toàn vẹn thông tin; xác định nguyên tắc thiết kế, triển khai vận hành các giao thức trao đổi, phân phối và quản lý khóa nhằm bảo đảm bí mật, xác thực, chống giả mạo và khả năng chống chịu trước các phương thức tấn công hiện đại. Hệ thống tiêu chuẩn, quy chuẩn kỹ thuật bao gồm các yêu cầu đối với sản phẩm mật mã, trong đó quy định tiêu chí chất lượng, độ an toàn, khả năng tương thích và điều kiện thử nghiệm, đánh giá, chứng nhận trước khi đưa vào sử dụng. Đối với khóa mã, hạ tầng quản lý khóa, tiêu chuẩn, quy chuẩn kỹ thuật quy định chặt chẽ về vòng đời khóa, cơ chế tạo, phân phối, lưu giữ, thay đổi và hủy bỏ khóa, nhằm bảo đảm an toàn liên tục trong suốt quá trình vận hành hệ thống mật mã.

Việc áp dụng thống nhất hệ thống tiêu chuẩn, quy chuẩn kỹ thuật này giúp bảo đảm tính liên thông giữa các hệ thống thông tin xử lý bí mật nhà nước của các cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc Việt Nam, các tổ chức chính trị và tổ chức chính trị - xã hội; hạn chế rủi ro khi sử dụng sản phẩm hoặc thuật toán không được kiểm chứng; tạo cơ sở để cập nhật, nâng cấp và tích hợp công nghệ mật mã tiên tiến, đáp ứng yêu cầu bảo mật ngày càng cao trong thời kỳ chuyển đổi số.

5.2. Hạ tầng mật mã: Đây là lớp gốc Khung kiến trúc hạ tầng mật mã quốc gia, được xây dựng dựa trên các tiêu chuẩn, quy chuẩn kỹ thuật, bảo đảm năng lực tính toán, kết nối, lưu trữ và an toàn kỹ thuật cho toàn hệ thống, đồng thời là lớp hạ tầng kỹ thuật phục vụ cho các ứng dụng và dịch vụ các lớp: Bảo mật, xác thực cho ứng dụng; Bảo mật dữ liệu và nền tảng lõi. Các thành phần chính:

5.2.1. Hệ thống chứng thực chữ ký số chuyên dùng công vụ: Hệ thống chứng thực chữ ký số chuyên dùng công vụ là nền tảng lõi về xác thực và chứng thực điện tử cho toàn bộ hệ thống chính trị do Ban Cơ yếu Chính phủ quản lý, vận hành. Hệ thống này cung cấp dịch vụ ký số, xác thực cho văn bản, dữ liệu, hồ sơ điện tử trong hoạt động hành chính, quản lý nhà nước. Tất cả các chứng thư chữ ký số chuyên dùng công vụ được phát hành, quản lý và thu hồi theo quy định pháp luật.

Hệ thống chứng thực chữ ký số chuyên dùng công vụ phải đáp ứng các yêu cầu kỹ thuật cao nhất về tính sẵn sàng, bao gồm việc đảm bảo thời gian phục hồi mục tiêu (RTO) và điểm phục hồi mục tiêu (RPO).

Hệ thống này được vận hành tại Trung tâm dữ liệu ngành cơ yếu và cơ yếu các bộ, ngành theo phân cấp, có cơ chế dự phòng nóng, giám sát an ninh theo thời gian thực; đồng thời được tích hợp chặt chẽ với các nền tảng chuyển đổi số trọng yếu của Chính phủ như: Trục tích hợp dữ liệu LGSP; Nền tảng tích hợp, chia sẻ dữ liệu quốc gia NDXP; Cổng dịch vụ công quốc gia; Trung tâm dữ liệu quốc gia..., nhằm bảo đảm mọi hoạt động ký số, xác thực và mã hóa được diễn ra liên tục trong môi trường số thống nhất.

5.2.2. Hệ thống quản lý khóa mật mã quốc gia: Quản lý tập trung toàn bộ vòng đời khóa mật mã (tạo, phân phối, lưu trữ, sao lưu, gia hạn, thu hồi, hủy bỏ khóa) cho toàn bộ hệ thống chính trị.

Mô hình vận hành: Vận hành theo mô hình "Quản lý khóa tập trung". Toàn bộ khóa mật mã được lưu trữ trong môi trường "vùng tin cậy" (Hardware Security Module - HSM) và được mã hóa bảo vệ bằng thuật toán mật mã của Ban Cơ yếu Chính phủ. Các Module HSM này bắt buộc phải tuân thủ các tiêu chuẩn bảo mật quốc tế nghiêm ngặt như FIPS 140-3 cấp độ 3 (Level 3) trở lên (hoặc các TCVN/QCVN tương đương) để bảo đảm khả năng chống giả mạo vật lý và bảo vệ khóa ở mức độ cao nhất.

Hệ thống được vận hành tại Trung tâm dữ liệu ngành cơ yếu và cơ yếu các bộ, ngành theo phân cấp, có cơ chế dự phòng nóng, giám sát an ninh theo thời gian thực.

5.2.3. Hệ thống giám sát sản phẩm, dịch vụ mật mã: Hệ thống có nhiệm vụ giám sát, phân tích, cảnh báo và xử lý các sự kiện an ninh liên quan đến hệ thống chứng thực chữ ký số chuyên dùng công vụ, hệ thống quản lý khóa mật mã quốc gia, các sản phẩm mật mã và các dịch vụ mật mã; được vận hành tại Trung tâm dữ liệu ngành Cơ yếu và Cơ yếu các Bộ, ngành theo phân cấp, có cơ chế dự phòng nóng, giám sát an ninh theo thời gian thực.

5.2.4. Trung tâm kiểm định sản phẩm mật mã: Trung tâm thực hiện kiểm định, thử nghiệm, giám định và chứng nhận hợp quy sản phẩm mật mã, sử dụng các giải pháp kiểm định theo chuẩn ISO/IEC 17025 (hoặc tương đương), có khả năng thực hiện phép đo, hiệu chuẩn và kiểm thử các mô-đun, thiết bị mật mã phần cứng và phần mềm bảo đảm tính khách quan, trung thực tuyệt đối.

5.2.5. Cơ sở đào tạo, nghiên cứu, phát triển sản phẩm, dịch vụ mật mã: Đây là lực lượng trực tiếp xây dựng nền tảng khoa học công nghệ mật mã, thông qua việc đào tạo đội ngũ chuyên gia có trình độ cao, nghiên cứu phát triển các thuật toán, thiết bị, giải pháp mật mã hiện đại và đánh giá, kiểm định an toàn các sản phẩm, dịch vụ mật mã. Sự phát triển của các cơ sở đào tạo không chỉ quyết định khả năng tự chủ công nghệ mật mã của quốc gia mà còn tạo động lực nâng cao năng lực phòng thủ số, bảo đảm cho hệ thống chính trị vận hành an toàn, tin cậy, bền vững trong kỷ nguyên dữ liệu và liên thông số.

5.2.6. Cơ sở sản xuất sản phẩm mật mã và trung tâm bảo đảm kỹ thuật mật mã: Giữ vai trò thiết yếu trong việc bảo đảm an toàn thông tin và duy trì hoạt động ổn định của các hệ thống có xử lý dữ liệu thuộc phạm vi bí mật nhà nước. Các cơ sở sản xuất sản phẩm mật mã có chức năng chủ yếu là tổ chức sản xuất, cung cấp các sản phẩm mật mã bảo vệ bí mật nhà nước theo quy định, đáp ứng kịp thời nhu cầu trang bị của các cơ quan, tổ chức trong hệ thống chính trị. Các trung tâm bảo đảm kỹ thuật thực hiện nhiệm vụ hỗ trợ triển khai, hướng dẫn sử dụng, xử lý sự cố, bảo trì, bảo dưỡng và sửa chữa sản phẩm mật mã, bảo đảm thiết bị luôn duy trì trạng thái hoạt động an toàn, thông suốt và ổn định. Ngoài ra, các đơn vị này có nhiệm vụ theo dõi tình trạng kỹ thuật của sản phẩm trong suốt quá trình sử dụng, đề xuất phương án nâng cấp, thay thế khi cần thiết; đồng thời phối hợp triển khai các biện pháp bảo đảm kỹ thuật phòng ngừa rủi ro, sự cố ảnh hưởng đến an toàn thông tin bí mật nhà nước.

5.2.7. Bảo mật kênh truyền: Bảo đảm an toàn cho dữ liệu trong quá trình trao đổi thông tin giữa các hệ thống thông tin trong toàn bộ hệ thống chính trị sử dụng các giải pháp bảo mật kênh truyền (thiết bị, phần mềm) bảo vệ thông tin tới cấp độ "Tối mật" do Ban Cơ yếu Chính phủ cung cấp.

5.2.8. Bảo mật nền tảng điện toán đám mây: Sử dụng mã hóa trong các thành phần của nền tảng điện toán đám mây nhằm bảo vệ dữ liệu ở mọi giai đoạn khi lưu trữ, truyền tải và xử lý bảo đảm tính bí mật, ngăn chặn truy cập trái phép. Các thành phần mật mã trong nền tảng điện toán đám mây sử dụng các giải pháp mã hóa theo tiêu chuẩn, quy chuẩn do ngành cơ yếu cung cấp để phát triển, tích hợp để bảo vệ các thông tin ở mức độ "Mật, Tối mật".

5.2.9. Bảo mật dữ liệu thiết bị đầu cuối: Bảo mật dữ liệu trên thiết bị đầu cuối là yêu cầu bắt buộc nhằm bảo đảm an toàn thông tin trong quá trình quản lý, lưu trữ và xử lý dữ liệu tại các cơ quan, tổ chức trong hệ thống chính trị. Việc bảo mật thiết bị đầu cuối được thực hiện theo nguyên tắc bảo đảm tính bí mật, toàn vẹn và sẵn sàng của dữ liệu; phòng ngừa, phát hiện và ngăn chặn các hành vi truy cập trái phép, cài cắm mã độc, đánh cắp hoặc làm sai lệch thông tin. Các biện pháp bảo mật thiết bị đầu cuối bao gồm mã hóa dữ liệu lưu trữ và dữ liệu trao đổi; áp dụng cơ chế xác thực mạnh; quản lý, bảo vệ khóa mật mã; thiết lập chế độ kiểm soát truy cập, phân quyền sử dụng và giám sát hoạt động trên thiết bị. Đồng thời, các cơ quan, tổ chức có trách nhiệm thực hiện cập nhật bản vá bảo mật, quản lý cấu hình, giám sát thiết bị ngoại vi, triển khai giải pháp phòng, chống mã độc và các công cụ giám sát an toàn phù hợp, bảo đảm thiết bị đầu cuối vận hành trong trạng thái an toàn theo quy định. Việc tăng cường bảo mật dữ liệu trên thiết bị đầu cuối góp phần bảo vệ thông tin bí mật nhà nước, thông tin quan trọng của cơ quan, tổ chức và nâng cao năng lực bảo đảm an ninh mạng trong bối cảnh chuyển đổi số.

5.3. Bảo mật dữ liệu và nền tảng lõi: Bảo vệ tính toàn vẹn, bí mật và xác thực của dữ liệu và nền tảng lõi trong suốt quá trình thu thập, xử lý, chia sẻ và lưu trữ dữ liệu. Các thành phần chính gồm:

5.3.1. Bảo mật dữ liệu lưu trữ: Sử dụng các giải pháp bảo mật dữ liệu cấp độ "Mật, Tối mật" đối với các cơ sở dữ liệu quốc gia và chuyên ngành phải bảo mật; nhằm ngăn ngừa rò rỉ, thất thoát thông tin, bảo đảm an toàn dữ liệu quan trọng phục vụ hoạt động của cơ quan, tổ chức trong bối cảnh chuyển đổi số. Dữ liệu phải được mã hóa tại ổ đĩa, tệp và cơ sở dữ liệu. Có cơ chế tách biệt người quản trị hệ thống và người nắm giữ khóa mã, tránh rủi ro nội bộ.

Các cơ quan có trách nhiệm áp dụng biện pháp bảo mật phù hợp như mã hóa dữ liệu, kiểm soát truy cập theo phân quyền, bảo vệ hệ thống lưu trữ, thực hiện sao lưu, phục hồi dữ liệu, đồng thời giám sát hoạt động truy xuất và quản lý chặt chẽ phương tiện lưu trữ theo quy định.

5.3.2. Bảo mật dữ liệu trên đường truyền: Là yêu cầu quan trọng nhằm bảo đảm an toàn cho thông tin trong quá trình trao đổi giữa các hệ thống, cơ quan, tổ chức trong toàn bộ hệ thống chính trị. Việc bảo mật dữ liệu truyền đưa được thực hiện theo nguyên tắc bảo đảm tính bí mật, toàn vẹn, xác thực và chống phủ nhận thông tin trong suốt quá trình truyền tải trên các môi trường mạng khác nhau.

Các cơ quan, tổ chức có trách nhiệm áp dụng các giải pháp bảo mật phù hợp do Ban Cơ yếu Chính phủ cung cấp bao gồm mã hóa dữ liệu trước khi truyền đưa; sử dụng các giao thức truyền thông an toàn; triển khai cơ chế xác thực hai chiều giữa các đầu mối truyền tin; giám sát và kiểm soát lưu lượng nhằm phát hiện, ngăn chặn các hành vi xâm nhập, giả mạo hoặc thay đổi dữ liệu; đồng thời, quản lý chặt chẽ khóa mật mã, bảo vệ thông số kỹ thuật liên quan và thực hiện định kỳ kiểm tra, đánh giá an toàn hệ thống thông tin bảo đảm theo đúng quy định pháp luật về bảo vệ bí mật nhà nước, cơ yếu và an ninh mạng.

5.3.3. Bảo mật dữ liệu khi sử dụng: Là yêu cầu trọng yếu nhằm bảo đảm an toàn thông tin trong suốt quá trình truy cập, xử lý và khai thác dữ liệu tại các cơ quan, tổ chức trong hệ thống chính trị; góp phần phòng ngừa nguy cơ rò rỉ thông tin từ bên trong, nâng cao trách nhiệm người dùng, bảo đảm dữ liệu luôn được xử lý trong môi trường an toàn, đáp ứng yêu cầu bảo mật trong bối cảnh chuyển đổi số và ứng dụng công nghệ thông tin trong hoạt động của các cơ quan, tổ chức.

Việc bảo mật dữ liệu khi sử dụng được thực hiện theo nguyên tắc bảo đảm chỉ những cá nhân, hệ thống và ứng dụng được phân quyền hợp lệ mới được truy cập và thao tác với dữ liệu, đồng thời mọi hoạt động sử dụng dữ liệu phải được kiểm soát, theo dõi và ghi nhận đầy đủ. Bảo mật nền tảng AI sử dụng mã hóa khi xử lý dữ liệu trong các thành phần của nền tảng AI nhằm bảo vệ dữ liệu luôn ở trạng thái mã hóa kể cả trong quá trình xử lý. Mọi dữ liệu huấn luyện nhạy cảm phải được ẩn danh và mã hóa trước khi đưa vào pipeline AI.

Các cơ quan, tổ chức có trách nhiệm áp dụng biện pháp kỹ thuật và quản lý phù hợp, bao gồm kiểm soát truy cập theo vai trò; sử dụng cơ chế xác thực mạnh; bảo vệ dữ liệu trong bộ nhớ và trong môi trường xử lý; hạn chế sao chép, xuất dữ liệu ra khỏi hệ thống; giám sát và phát hiện hành vi bất thường trong quá trình sử dụng; đồng thời, quản lý chặt chẽ nhật ký truy cập, thiết lập chính sách phân quyền chi tiết và triển khai các giải pháp bảo vệ ứng dụng bảo đảm theo đúng quy định pháp luật về bảo vệ bí mật nhà nước, cơ yếu và an ninh mạng.

5.4. Bảo mật, xác thực cho ứng dụng

5.4.1. Dịch vụ ký số/xác thực: Bảo đảm tính pháp lý, an toàn và tin cậy cho mọi văn bản, hồ sơ và giao dịch điện tử trong các cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc Việt Nam, các tổ chức chính trị và tổ chức chính trị - xã hội từ Trung ương đến địa phương. Dịch vụ do Ban Cơ yếu Chính phủ cung cấp, có thể tích hợp với các hệ thống quản lý văn bản, văn bản mật, điều hành, cổng dịch vụ công, hệ thống nhân sự, tài chính,... Các yêu cầu thực hiện theo quy định pháp luật hiện hành về chữ ký số chuyên dùng công vụ.

5.4.2. Dịch vụ mã hóa, bảo mật dữ liệu: Cung cấp dịch vụ mã hóa, giải mã, quản lý khóa và kiểm soát truy cập dữ liệu cho các ứng dụng trong toàn bộ hệ thống chính trị. Thay vì mỗi hệ thống phải tự cài đặt giải pháp bảo mật riêng, các cơ quan có thể sử dụng API mã hóa do Ban Cơ yếu Chính phủ cung cấp. Cơ chế mã hóa lớp ứng dụng sử dụng khóa dữ liệu và khóa mã hóa chính được quản lý bởi hệ thống quản lý khóa mật mã quốc gia. Tất cả các thao tác mã hóa/giải mã được thực hiện thông qua API chuẩn có xác thực, ký số và kiểm soát truy cập. Dữ liệu được bảo vệ ở ba trạng thái: khi lưu trữ, khi truyền và khi xử lý.

5.5. Chính sách, quy trình: Hệ thống chính sách và quy trình trong Khung kiến trúc hạ tầng mật mã quốc gia bảo đảm các hoạt động liên quan đến mật mã được triển khai nhất quán, có kiểm soát và phù hợp với đặc thù từng cơ quan, tổ chức. Đây là cơ sở để tăng cường quản lý nhà nước về mật mã, hạn chế rủi ro trong vận hành, nâng cao hiệu quả bảo vệ thông tin bí mật nhà nước và đóng góp vào năng lực phòng thủ mạng của toàn bộ hệ thống chính trị.

5.5.1. Chính sách: Các chính sách về mật mã được ban hành nhằm thiết lập khuôn khổ quản lý thống nhất, bảo đảm mọi hoạt động ứng dụng và triển khai mật mã tuân thủ pháp luật về bảo vệ bí mật nhà nước và pháp luật về cơ yếu. Một số chính sách chủ yếu gồm:

- Chính sách quản lý, sử dụng mật mã: Quy định nguyên tắc sử dụng mật mã cho các hệ thống thông tin theo cấp độ mật; xác định phạm vi, đối tượng và trách nhiệm của các cơ quan, tổ chức trong triển khai, vận hành các giải pháp mật mã.

- Chính sách về tiêu chuẩn, quy chuẩn mật mã: Xác định yêu cầu kỹ thuật tối thiểu đối với giao thức, thuật toán, khóa mã, sản phẩm mật mã; quy định trách nhiệm tuân thủ và cơ chế áp dụng trong các hệ thống thông tin.

- Chính sách quản lý khóa mật mã: Quy định phương pháp tạo, phân phối, lưu giữ, thay đổi và hủy bỏ khóa; yêu cầu về bảo vệ khóa trong suốt vòng đời và trách nhiệm của các đơn vị liên quan.

- Chính sách quản lý sản phẩm mật mã: Quy định về kiểm tra, đánh giá, chứng nhận, nghiệm thu và kiểm soát sử dụng sản phẩm mật mã trong các cơ quan, tổ chức.

- Chính sách bảo vệ thông tin bí mật nhà nước trong môi trường số: Xác định các mức độ bảo vệ, cơ chế kiểm soát truy cập, phân quyền, giám sát và xử lý dữ liệu bí mật nhà nước.

- Chính sách về đào tạo, kiểm tra và giám sát an toàn mật mã: Định hướng đào tạo, bồi dưỡng năng lực chuyên môn cho người trực tiếp quản lý, triển khai, sử dụng mật mã; quy định về kiểm tra, đánh giá định kỳ và đột xuất.

5.5.2. Quy trình: Các quy trình kỹ thuật, nghiệp vụ được xây dựng nhằm hướng dẫn cụ thể việc triển khai, vận hành và kiểm soát các hoạt động liên quan đến mật mã. Một số quy trình chính bao gồm:

- Quy trình quản lý vòng đời khóa mật mã: Bao gồm tạo khóa, phân phối, lưu giữ, thay đổi định kỳ, thu hồi và hủy khóa theo đúng quy định, bảo đảm an toàn ở tất cả các giai đoạn.

- Quy trình quản lý vòng đời sản phẩm mật mã: Từ kiểm tra, đánh giá, chứng nhận, mua sắm, triển khai thực hiện đến bảo trì, thay thế, thu hồi và tiêu hủy sản phẩm mật mã, bảo đảm sản phẩm được sử dụng đúng mục đích, đúng phạm vi.

- Quy trình mã hóa, giải mã dữ liệu: Quy định các bước thực hiện mã hóa, giải mã, kiểm soát truy cập, ghi nhật ký và bảo đảm an toàn cho quá trình xử lý dữ liệu.

- Quy trình phân phối và trao đổi khóa: Xác định phương pháp, giao thức và yêu cầu an toàn đối với quá trình trao đổi khóa giữa các hệ thống hoặc các cơ quan.

- Quy trình vận hành, giám sát và kiểm tra an toàn mật mã: Bao gồm giám sát hoạt động hệ thống mật mã, phát hiện bất thường, kiểm tra an toàn định kỳ, kiểm thử xâm nhập và đánh giá mức độ bảo mật.

- Quy trình quản lý sự cố liên quan đến mật mã: Xác định phương án tiếp nhận, phân loại, xử lý, khắc phục sự cố và báo cáo theo đúng thẩm quyền.

- Quy trình bảo vệ dữ liệu mật mã trong môi trường lưu trữ, sử dụng và truyền đưa: Quy định phương pháp mã hóa, phân quyền, kiểm soát truy cập và giám sát toàn bộ vòng đời dữ liệu.

6. Nguyên tắc triển khai, vận hành và giám sát

6.1. Nguyên tắc tổng thể: Khung kiến trúc hạ tầng mật mã quốc gia được triển khai và vận hành theo nguyên tắc "an toàn - thống nhất - linh hoạt - liên thông - kiểm soát toàn vòng đời", bảo đảm gắn kết chặt chẽ giữa hạ tầng kỹ thuật, hành lang pháp lý và năng lực quản trị. Tất cả hoạt động trong hệ sinh thái mật mã từ thiết kế, triển khai, khai thác đến giám sát, phải tuân thủ chuẩn kỹ thuật quốc gia, phù hợp thông lệ quốc tế, đồng thời bảo đảm chủ quyền mật mã, tự chủ công nghệ của các cơ quan, tổ chức thuộc hệ thống chính trị.

Nguyên tắc triển khai và vận hành Khung kiến trúc hạ tầng mật mã quốc gia được đặt trên nền tảng tư duy: "Mật mã là lớp bảo mật lõi của an ninh số quốc gia, vừa bảo vệ, vừa thúc đẩy chuyển đổi số". Hệ thống phải vận hành ổn định, tự chủ công nghệ, giám sát chủ động, tương thích quốc tế, góp phần hình thành một không gian số an toàn, tin cậy và có chủ quyền của Việt Nam.

6.2. Nguyên tắc triển khai: Triển khai theo lớp và đồng bộ trong toàn hệ thống chính trị. Việc triển khai phải đồng bộ giữa các khối: Cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc Việt Nam, các tổ chức chính trị và tổ chức chính trị - xã hội từ Trung ương đến địa phương bảo đảm tương thích, tránh trùng lặp đầu tư và tuân thủ nguyên tắc "một chuẩn - nhiều ứng dụng". Bảo đảm phân tầng bảo mật và phân cấp quản trị rõ ràng theo mức độ mật và phạm vi sử dụng. Kết hợp nguồn lực và chia sẻ trách nhiệm đa cơ quan, Ban Cơ yếu Chính phủ đóng vai trò chủ trì kỹ thuật và tiêu chuẩn, quy chuẩn kỹ thuật; các ban, bộ, ngành, địa phương chịu trách nhiệm triển khai thực hiện trong phạm vi quản lý.

6.3. Nguyên tắc vận hành: Vận hành theo cơ chế "phân tầng - phân quyền - liên thông an toàn". Mỗi lớp, mỗi thành phần trong Khung kiến trúc hạ tầng mật mã quốc gia đều có chức năng vận hành rõ ràng, được kiểm định định kỳ. Giám sát thời gian thực và phản ứng chủ động, toàn bộ hệ thống được kết nối với hệ thống giám sát sản phẩm, dịch vụ mật mã quốc gia, nơi thu thập, phân tích, cảnh báo và xử lý các sự kiện bất thường. Hạ tầng mật mã phải được đánh giá an ninh, an toàn ít nhất 1 lần/năm bởi cơ quan do Ban Cơ yếu Chính phủ chỉ định. Các sản phẩm mật mã, thiết bị HSM, thuật toán, giao thức và phần mềm mã hóa phải đạt các tiêu chuẩn, quy chuẩn kỹ thuật do Ban Cơ yếu Chính phủ xây dựng, TCVN/ISO/IEC 19790,… Công tác bảo trì, cập nhật khóa và chính sách được tự động hóa ở mức cao để giảm thiểu rủi ro con người.

6.4. Nguyên tắc giám sát và đánh giá

6.4.1. Giám sát đa tầng, đa chiều, hệ thống giám sát được thiết kế 3 tầng liên kết

- Tầng cơ sở: Đơn vị vận hành hệ thống chứng thực chữ ký số chuyên dùng công vụ, hệ thống quản lý khóa mật mã quốc gia, hạ tầng mạng mật quốc gia.

- Tầng ngành/lĩnh vực: Cơ quan chủ quản (ví dụ: Bộ Công an, Bộ Quốc phòng, Bộ Khoa học và Công nghệ) tổng hợp, đánh giá tuân thủ.

- Tầng quốc gia: Hệ thống giám sát dịch vụ, sản phẩm mật mã quốc gia thuộc Ban Cơ yếu Chính phủ phân tích tổng hợp, phát hiện rủi ro hệ thống, phát hành cảnh báo toàn mạng.

6.4.2. Đánh giá định kỳ và đột xuất

- Định kỳ hằng năm: Đánh giá toàn vẹn, tính sẵn sàng và an toàn hệ thống, cập nhật tiêu chuẩn thuật toán, khóa, chứng thư.

- Đột xuất: Kích hoạt khi có sự cố, vi phạm, hoặc phát hiện bất thường trong mạng lưới mật mã.

6.4.3. Nguyên tắc giám sát: Hệ thống giám sát phân tích chuỗi sự kiện bất thường và dự báo tấn công mã hóa giả mạo. Các log giám sát được bảo đảm không thể chỉnh sửa sau khi ghi nhận.

6.4.4. Trách nhiệm và minh bạch: Mọi cơ quan, tổ chức sử dụng hoặc vận hành hạ tầng mật mã quốc gia phải tuân thủ chế độ báo cáo, đánh giá định kỳ; chịu trách nhiệm trước pháp luật nếu để xảy ra vi phạm, rò rỉ thông tin hoặc mất an toàn dữ liệu thông tin bí mật nhà nước.

II. MÔ HÌNH KHUNG KIẾN TRÚC HẠ TẦNG MẬT MÃ QUỐC GIA ÁP DỤNG CHO MÔ HÌNH LIÊN THÔNG SỐ THỐNG NHẤT, HIỆU QUẢ VÀ QUẢN TRỊ DỰA TRÊN DỮ LIỆU TRONG HỆ THỐNG CHÍNH TRỊ

1. Mục đích: Xây dựng mô hình áp dụng Khung kiến trúc hạ tầng mật mã quốc gia theo Quy định số 05-QĐ/BCĐTW của Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số (Quy định số 05) về mô hình liên thông số thống nhất, hiệu quả và quản trị dựa trên dữ liệu trong hệ thống chính trị, đồng bộ với Khung kiến trúc tổng thể quốc gia số, Khung kiến trúc dữ liệu quốc gia, Khung quản trị, quản lý dữ liệu quốc gia, Từ điển dữ liệu dùng chung đóng vai trò là lớp bảo mật hạ tầng lõi, cung cấp dịch vụ mã hóa, ký số, xác thực cho các hệ thống thông tin và nền tảng số trọng yếu của quốc gia.

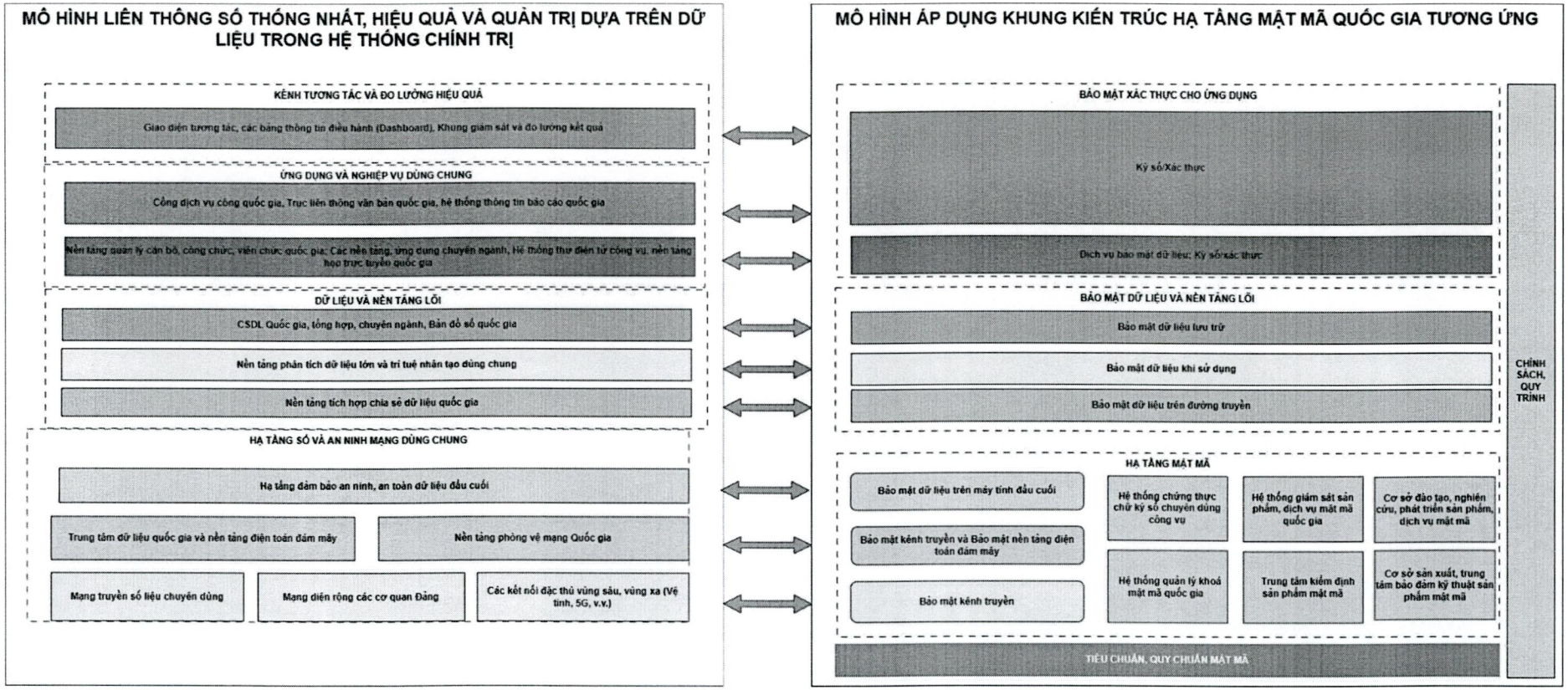
2. Nguyên tắc xây dựng: Mô hình Khung kiến trúc hạ tầng mật mã quốc gia áp dụng cho Mô hình liên thông số thống nhất, hiệu quả và quản trị dựa trên dữ liệu trong hệ thống chính trị được xây dựng theo tư duy kiến trúc hệ thống tổng thể, đặt trọng tâm vào sự đồng bộ với Quy định số 05, liên thông dữ liệu, tạo ra lớp bảo mật lõi cho hạ tầng số quốc gia và được xây dựng theo nguyên tắc:

- Phân chia thành các lớp chức năng rõ ràng, phù hợp, đồng bộ với Mô hình liên thông số thống nhất, hiệu quả và quản trị dựa trên dữ liệu trong hệ thống chính trị theo Quy định số 05.

- Kế thừa thực tiễn triển khai, chuẩn hóa và tích hợp các hạ tầng mật mã hiện có từ Trung ương tới các ban, bộ, ngành, địa phương.

- Liên thông và tích hợp: Bảo đảm các yếu tố kết nối, chia sẻ, xác thực thống nhất và liên thông, bảo đảm dữ liệu an toàn, không trùng lặp và dễ dàng kiểm soát xuyên suốt giữa các cơ quan, cấp chính quyền và lĩnh vực.

3. Mô hình Khung kiến trúc hạ tầng mật mã quốc gia áp dụng cho mô hình liên thông số thống nhất, hiệu quả và quản trị dựa trên dữ liệu trong hệ thống chính trị



Hình 2. Mô hình Khung kiến trúc hạ tầng mật mã quốc gia áp dụng cho Mô hình liên thông số thống nhất, hiệu quả và quản trị dựa trên dữ liệu trong hệ thống chính trị

3.1. Lớp kênh tương tác và đo lường hiệu quả

Thành phần mô hình liên thông số	Thành phần Khung mật mã tương ứng	Nội dung áp dụng
Các giao diện tương tác, bảng thông tin điều hành, dashboard, khung giám sát và đo lường kết quả	Ký số/xác thực	Bảo đảm tính xác thực, toàn vẹn và chống giả mạo dữ liệu phục vụ chỉ đạo, điều hành

3.2. Lớp ứng dụng và nghiệp vụ dùng chung

Thành phần mô hình liên thông số	Thành phần Khung mật mã tương ứng	Nội dung áp dụng
Cổng dịch vụ công quốc gia, trục liên thông văn bản quốc gia, hệ thống thông tin báo cáo quốc gia	Ký số/xác thực	Bảo đảm tính xác thực, toàn vẹn và chống giả mạo dữ liệu phục vụ chỉ đạo, điều hành
Các nền tảng quản lý cán bộ, công chức, viên chức; nền tảng ứng dụng chuyên ngành; hệ thống thư điện tử công vụ; nền tảng họp trực tuyến quốc gia	Dịch vụ bảo mật dữ liệu; ký số/xác thực	Bảo vệ dữ liệu nhạy cảm trong quá trình truy cập, xử lý; bảo đảm tính xác thực, toàn vẹn các văn bản, tài liệu, trao đổi trực tuyến

3.3. Lớp dữ liệu và nền tảng lõi

Thành phần mô hình liên thông số	Thành phần Khung mật mã tương ứng	Nội dung áp dụng
Cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành, bản đồ số quốc gia	Bảo mật dữ liệu lưu trữ	Mã hóa dữ liệu lưu trữ; kiểm soát truy cập theo cấp độ bảo mật
Nền tảng phân tích dữ liệu lớn và trí tuệ nhân tạo	Bảo mật dữ liệu khi sử dụng	Bảo vệ dữ liệu trong bộ nhớ và quá trình xử lý; hạn chế rò rỉ dữ liệu nội bộ

Thành phần mô hình liên thông số	Thành phần Khung mật mã tương ứng	Nội dung áp dụng
Nền tảng tích hợp chia sẻ dữ liệu quốc gia	Bảo mật dữ liệu trên đường truyền	Mã hóa, xác thực hai chiều; bảo đảm an toàn trao đổi dữ liệu liên thông

3.4. Lớp hạ tầng số và an ninh mạng dùng chung

Thành phần mô hình liên thông số	Thành phần Khung mật mã tương ứng	Nội dung áp dụng
Trung tâm dữ liệu quốc gia và nền tảng điện toán đám mây, Nền tảng phòng vệ mạng quốc gia	Bảo mật kênh truyền/ Bảo mật nền tảng điện toán đám mây	Bảo vệ các kết nối hệ thống trọng yếu và dữ liệu trao đổi giữa các cụm trung tâm dữ liệu
Mạng truyền số liệu chuyên dùng; Mạng thông tin diện rộng của Đảng; Các kết nối đặc thù vùng sâu, vùng xa (vệ tinh, 5G,…)	Bảo mật kênh truyền	Mã hóa dữ liệu, bảo đảm an toàn cho các kết nối chuyên dùng của cơ quan Đảng, Nhà nước
Hạ tầng bảo đảm an ninh, an toàn dữ liệu đầu cuối	Bảo mật dữ liệu trên máy tính đầu cuối	Mã hóa, bảo đảm an toàn cho dữ liệu khi được lưu trữ, xử lý trên các thiết bị đầu cuối

3.5. Lớp chính sách, quy trình và tiêu chuẩn, quy chuẩn kỹ thuật mật mã

Thành phần mô hình liên thông số	Thành phần Khung mật mã tương ứng	Nội dung áp dụng
Tuân thủ và cập nhật yêu cầu kỹ thuật và công nghệ	Chính sách và quy trình mật mã	Quy định sử dụng, quản lý thiết bị mật mã, quản lý khóa, vận hành và kiểm tra an toàn mật mã
Tuân thủ và cập nhật yêu cầu kỹ thuật và công nghệ	Tiêu chuẩn, quy chuẩn kỹ thuật mật mã	Bảo đảm triển khai thống nhất theo tiêu chuẩn quốc gia, tuân thủ pháp luật về bảo vệ bí mật nhà nước

III. TỔ CHỨC THỰC HIỆN

1. Lộ trình triển khai

1.1. Giai đoạn 2025 - 2026: Tạo lập nền tảng Khung kiến trúc hạ tầng mật mã quốc gia

- Hoàn thiện khung pháp lý, tiêu chuẩn kỹ thuật và mô hình quản trị.

- Xây dựng và vận hành mạng mật quốc gia, mở rộng triển khai tới các bộ, ngành, địa phương, tổ chức chính trị - xã hội.

- Chuẩn hóa các thuật toán, giao thức và thiết bị mật mã bảo đảm tính thống nhất, liên thông, đồng bộ trong toàn bộ hệ thống chính trị.

- Thiết kế hệ thống quản lý khóa mật mã quốc gia.

- Thiết kế hệ thống giám sát sản phẩm, dịch vụ mật mã quốc gia.

1.2. Giai đoạn 2027 - 2028: Xây dựng hoàn thiện hạ tầng mật mã quốc gia

- Xây dựng hệ thống quản lý khóa mật mã quốc gia.

- Xây dựng hệ thống giám sát sản phẩm, dịch vụ mật mã quốc gia.

- Hoàn thiện trung tâm kiểm định sản phẩm mật mã.

- Triển khai và tích hợp 100% các API dịch vụ dùng chung.

- Triển khai thử nghiệm mật mã hậu lượng tử.

1.3. Giai đoạn 2029 - 2030: Tối ưu và chuyển đổi hậu lượng tử

- Sử dụng mật mã hậu lượng tử thay thế toàn diện mật mã truyền thống.

- Tích hợp toàn diện với nền tảng Chính phủ số, kinh tế số và xã hội số.

- Tham gia các Điều ước quốc tế về công nghệ mật mã, bảo vệ dữ liệu và định danh số.

2. Tổ chức triển khai

2.1. Nguyên tắc chung

Khung kiến trúc hạ tầng mật mã quốc gia được triển khai trên cơ sở thống nhất quản lý, phân cấp vận hành, phối hợp liên ngành và giám sát tập trung, bảo đảm sự tham gia đầy đủ các cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội từ Trung ương đến địa phương.

Tất cả các cơ quan, tổ chức trong hệ thống chính trị có trách nhiệm triển khai kết nối vào Mạng mật liên thông các cơ quan trong hệ thống chính trị để gửi, nhận, xử lý, lưu trữ và trao đổi văn bản, hồ sơ công việc cấp độ Mật, Tối mật bảo đảm liên thông, thống nhất và an ninh, an toàn.

Toàn bộ hoạt động liên quan đến mật mã để bảo vệ thông tin bí mật nhà nước phải tuân thủ đúng quy định của pháp luật về bảo vệ bí mật nhà nước, cơ yếu và an ninh mạng.

2.2. Trách nhiệm của Ban Cơ yếu Chính phủ

- Giúp Bộ trưởng Bộ Quốc phòng thực hiện quản lý nhà nước về mật mã, chỉ đạo, giám sát và tổ chức triển khai toàn bộ Khung kiến trúc hạ tầng mật mã quốc gia.

- Xây dựng, quản lý và vận hành: Hệ thống quản lý khóa mật mã quốc gia; Hệ thống chứng thực chữ ký số chuyên dùng công vụ; Hệ thống bảo mật cho Mạng mật liên thông các cơ quan trong hệ thống chính trị phục vụ trao đổi, gửi nhận văn bản, hồ sơ công việc đến cấp độ Mật, Tối mật; Hệ thống giám sát sản phẩm, dịch vụ mật mã quốc gia; Trung tâm kiểm định sản phẩm mật mã;

- Chủ trì xây dựng, cung cấp các API dịch vụ dùng chung (ký số, mã hóa, xác thực).

- Xây dựng và trình Bộ trưởng Bộ Quốc phòng ban hành các TCVN/QCVN về thuật toán, giao thức, sản phẩm mật mã.

- Thực hiện thẩm định, kiểm định, đánh giá và giám sát tuân thủ mật mã trong tất cả các đề án, dự án chuyển đổi số quốc gia.

- Tổ chức đào tạo, tập huấn về Khung kiến trúc hạ tầng mật mã quốc gia.

- Là đầu mối hợp tác quốc tế trong lĩnh vực mật mã, tiêu chuẩn hóa, kiểm định và công nghệ hậu lượng tử.

- Thường xuyên rà soát, đề xuất sửa đổi, bổ sung nội dung Khung kiến trúc hạ tầng mật mã quốc gia nhằm đáp ứng yêu cầu bảo đảm an toàn, bí mật và toàn vẹn cho các hoạt động xử lý, lưu trữ và trao đổi thông tin của các cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội từ Trung ương đến địa phương.

2.3. Trách nhiệm của các cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc Việt Nam, các tổ chức chính trị và tổ chức chính trị - xã hội từ Trung ương tới địa phương

- Tuân thủ Khung kiến trúc hạ tầng mật mã quốc gia.

- Chủ trì, phối hợp với Ban Cơ yếu Chính phủ triển khai các giải pháp bảo mật và tích hợp các API dịch vụ dùng chung (ký số, mã hóa, xác thực) vào các hệ thống thông tin nghiệp vụ.

- Kết nối vào mạng mật dựa trên hạ tầng mạng thông tin diện rộng của Đảng phục vụ trao đổi, xử lý văn bản, dữ liệu, hồ sơ công việc đến cấp độ Mật, Tối mật.