| BAN CƠ YẾU CHÍNH PHỦ | CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM<br>Độc lập - Tự do - Hạnh phúc |
|---|---|
| Số: 14/2018/GPKD-BCY | *Hà Nội, ngày 24 tháng 4 năm 2018* |

# GIẤY PHÉP
## KINH DOANH SẢN PHẨM, DỊCH VỤ MẬT MÃ DÂN SỰ

### TRƯỞNG BAN BAN CƠ YẾU CHÍNH PHỦ

Căn cứ Luật an toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 58/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ quy định chi tiết về kinh doanh sản phẩm, dịch vụ mật mã dân sự và xuất khẩu, nhập khẩu sản phẩm mật mã dân sự;

Xét hồ sơ đề nghị cấp bổ sung Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự của **Công ty Cổ phần Chữ ký số VI NA**;

Theo đề nghị của Cục trưởng Cục Quản lý mật mã dân sự và Kiểm định sản phẩm mật mã,

## QUYẾT ĐỊNH:

**Điều 1. CÔNG TY CỔ PHẦN CHỮ KÝ SỐ VI NA.**

Địa chỉ trụ sở chính: **Số 41A Nguyễn Phi Khanh, Phường Tân Định, Quận 1, Thành phố Hồ Chí Minh, Việt Nam**

Điện thoại: **028.38202261**

Giấy chứng nhận đăng ký doanh nghiệp, mã số doanh nghiệp: 0309612872 do Sở Kế hoạch và Đầu tư thành phố Hồ Chí Minh cấp đăng ký lần đầu ngày 09 tháng 12 năm 2009, đăng ký thay đổi lần thứ 8 ngày 22 tháng 7 năm 2014.

Được kinh doanh sản phẩm, dịch vụ mật mã dân sự theo Danh mục kèm theo Giấy phép này.

**Điều 2. Công ty Cổ phần Chữ ký số VI NA** phải thực hiện đúng các quy định của Luật an toàn thông tin mạng và Nghị định số 58/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ quy định chi tiết về kinh doanh sản phẩm, dịch vụ mật mã dân sự và xuất khẩu, nhập khẩu sản phẩm mật mã dân sự.

**Điều 3.** Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự này có thời hạn từ ngày 24 tháng 4 năm 2018 đến hết ngày 24 tháng 4 năm 2028./.

***Nơi nhận:***
- Như Điều 1;
- Lưu: VT, MMDSKĐ; L03.

**TRƯỞNG BAN**

**Đặng Vũ Sơn**

**DANH MỤC CÁC SẢN PHẨM, DỊCH VỤ MẬT MÃ DÂN SỰ ĐƯỢC PHÉP KINH DOANH**

*(Kèm theo Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự số 14/2018/GPKD-BCY ngày 24/4/2018 của Ban Cơ yếu Chính phủ)*

## I. Danh mục sản phẩm mật mã dân sự được phép kinh doanh

| STT | Tên nhóm sản phẩm | Tiêu chuẩn, đặc tính kỹ thuật | Phạm vi, lĩnh vực cung cấp |
|---|---|---|---|
| **I** | **Sản phẩm bảo mật dữ liệu lưu giữ** | | |
| 1 | SDencrypter | - Thuật toán mã hóa: 3DES, AES (128 bit, 192 bit, 256 bit) RSA (1024 bit, 2048 bit, 3072 bit).<br>- Hàm băm mật mã: SHA-1, SHA-256.<br>- HMAC: HMAC-SHA1, HMAC-SHA256.<br>Chứng chỉ: FIPS 140-2 Level 3. | Để bảo vệ thông tin không thuộc phạm vi bí mật nhà nước;<br>Cung cấp cho các tổ chức, cá nhân trong các lĩnh vực: Tài chính; Bảo hiểm; Bưu chính viễn thông; Giao thông vận tải; Doanh nghiệp, cơ quan nhà nước. |
| 2 | Hệ thống quản lý xác thực hàng hóa sử dụng tem chống hàng giả Vina | - Thuật toán mã hóa: AES (128 bit)<br>- Khóa mật mã: Sinh khóa theo thuật toán của Công ty Chữ ký số Vina với mầm khóa là mật khẩu của người dùng.<br>- Chức năng phần mềm: Quản lý và xác thực hàng hóa sử dụng tem nhãn xác thực có bảo mật; mã hóa cơ sở dữ liệu, vùng đĩa, file. | |
| **II** | **Thành phần mật mã trong hệ thống PKI** | | |
| 1 | SecurityServer Se-Series bao gồm các dòng: Se10/ Se50/ Se400/ Se1000. | - Thuật toán mã hóa phi đối xứng: RSA độ dài khóa (1024 bit, 1536 bit, 2048 bit, 3072 bit, 4096 bit), ECDSA, DSA độ dài khóa (1024 bit, 2048 bit).<br>- Thuật toán mã hóa đối xứng: AES chế độ (ECB, CBC, CFB8, OFB, CMAC, GCM) độ dài khóa (128 bit, 192 bit, 256 bit), Triple-DES chế độ (CBC, EBC).<br>- Hàm băm mật mã: SHA-1, SHA- | |

| STT | Tên nhóm sản phẩm | Tiêu chuẩn, đặc tính kỹ thuật | Phạm vi, lĩnh vực cung cấp |
|---|---|---|---|
| | | 224, SHA-256, SHA-384, SHA-512.<br>- Mã xác thực thông báo: HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512.<br>- Tiêu chuẩn áp dụng: PKCS#11<br>- Chứng chỉ: FIPS 140-2 level 3. | Để bảo vệ thông tin không thuộc phạm vi bí mật nhà nước;<br>Cung cấp cho các tổ chức, cá nhân trong các lĩnh vực: Tài chính; Bảo hiểm; Bưu chính, Viễn thông; Giao thông vận tải; Doanh nghiệp, cơ quan nhà nước. |
| 2 | SecureMetric ST3ACE Token | - Thuật toán mã hóa phi đối xứng: RSA độ dài khóa (1024 bit, 2048 bit)<br>- Thuật toán mã hóa đối xứng: AES độ dài khóa (128 bit) chế độ (CBC, ECB), Triple-DES chế độ (CBC, ECB)<br>- Hàm băm mật mã: SHA-1, SHA-256<br>- Sinh số ngẫu nhiên tuân theo tiêu chuẩn NIST SP 800-90<br>- Hỗ trợ PKCS#1v1.5<br>- Chứng chỉ: FIPS 140-2 level 3 | |
| 3 | FEITIAN ePass2003 Token | - Thuật toán mã hóa phi đối xứng: RSA độ dài khóa (1024 bit, 2048 bit), ECDSA độ dài khóa (192 bit, 256 bit)<br>- Thuật toán mã hóa đối xứng: AES độ dài khóa (128 bit) chế độ (CBC, ECB), Triple-DES chế độ (CBC, ECB)<br>- Hàm băm mật mã: SHA-1, SHA-256<br>- Sinh số ngẫu nhiên tuân theo tiêu chuẩn NIST SP 800-90<br>- Hỗ trợ: PKCS#11<br>- Chứng chỉ: FIPS 140-2 level 3, Comcom Criteria EAL 5+ | |

## II. Danh mục dịch vụ mật mã dân sự được phép kinh doanh

| STT | Tên dịch vụ | Phạm vi, lĩnh vực cung cấp |
|---|---|---|
| 1 | Dịch vụ kiểm định, đánh giá sản phẩm mật mã dân sự | Để bảo vệ thông tin không thuộc phạm vi bí mật nhà nước;<br>Cung cấp cho các tổ chức, cá nhân trong các lĩnh vực: Tài chính; Bảo hiểm; Bưu chính, Viễn thông; Giao thông vận tải; Doanh nghiệp, cơ quan nhà nước. |
| 2 | Dịch vụ tư vấn bảo mật, an toàn thông tin mạng sử dụng sản phẩm mật mã dân sự | |