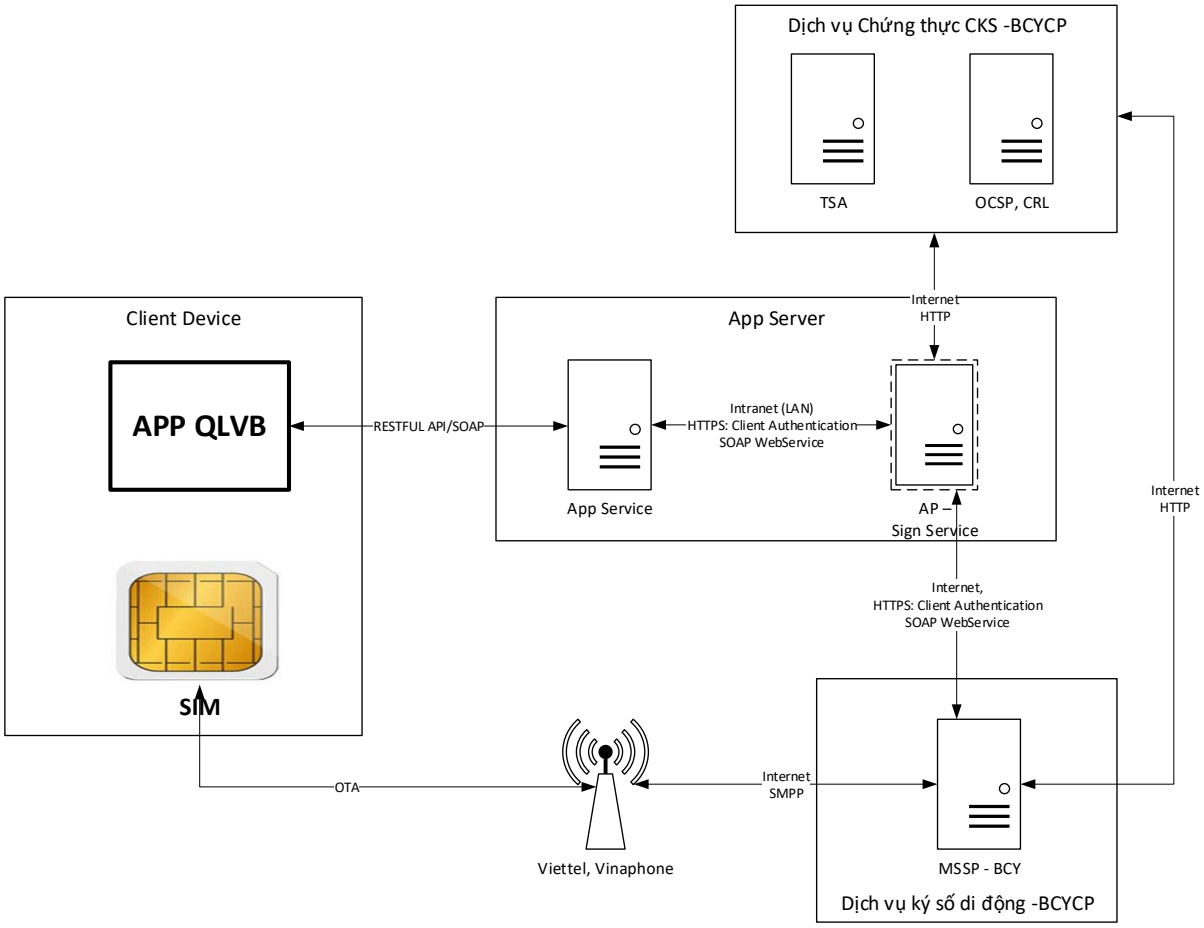
Hướng dẫn tích hợp chữ ký số sử dụng SIM-PKI

1. Giới thiệu chung về giải pháp tích hợp ký số cho ứng dụng di động

1.1. Mô hình hệ thống



Trong mô hình trên AP Sign Service (AP) là máy chủ dịch vụ hỗ trợ ký số trên thiết bị di động. Máy chủ dịch vụ AP sẽ kết nối đến dịch vụ ký số di động (MSSP) của Ban Cơ yếu Chính phủ để gửi yêu cầu ký số đến SIM-PKI và nhận kết quả ký số sau đó đóng gói theo định dạng chữ ký số PDF. Ngoài ra, máy chủ dịch vụ AP kết nối đến các dịch vụ chứng thực của hệ thống CA chuyên dùng Chính phủ để kiểm tra chứng thư số (OCSP, CRLs) và để tích hợp dịch vụ cấp dấu thời gian (TSA) trong quá trình ký số và kiểm tra chữ ký số.

1.2. Yêu cầu về phần mềm

- Phần mềm hỗ trợ tích hợp ký số cho ứng dụng di động mpkicrypto-v1.0.x, bao gồm:

+ Thư viện tích hợp ký số tệp PDF sử dụng SIM-PKI: MPKICrypto.dll

+ ASP.NET WebSerivce tích hợp thư viện MPKICrypto: MPKIWebService. WebService cung cấp API ký PDF tự động xác định vị trí chữ ký theo mẫu dự thảo công văn hoặc ký số PDF với vị trí được xác định trước.

- Bộ công cụ tích hợp được xây dựng trên .Net Framework 4.5

- WebService ký số chạy trên WebServer IIS 8.5

1.3. Yêu cầu về phần cứng máy chủ dịch vụ AP

- Phần cứng máy chủ dịch vụ AP có thể theo lựa chọn dưới đây, hoặc tương đương:

Hệ điều hành	Windows Server 2012
CPU, RAM, Hard drive, etc	CPU: 1 x Intel® Xeon-Silver 4110 (2.1GHz/8-core/85W)
	Memory: 2 x 16 GB RDIMM DR 2600 MT/s (2 x 16 GB)
	Hard drive: Intel D3-S4510 960GB, SATA 6Gb/s, 3D, TLC 2.5", 7.0mm
	Network Controller: 1Gb Ethernet 2-Port 331i Adapter plus

2. Chi tiết thư viện hỗ trợ tích hợp MPKICrypto.dll

2.1. Các lớp chính của thư viện

- PdfSigner: Lớp thực hiện chức năng ký số PDF

- PdfVerifier: Lớp thực hiện chức năng xác thực PDF

2.2. Các thành phần của lớp PdfSigner

a. Các thuộc tính:

Tên thuộc tính	**Kiểu dữ liệu**	**Ghi chú**
InputPdf	String	Đường dẫn tệp PDF đầu vào để ký số
OutputPdf	String	Đường dẫn tệp PDF đã ký số
Cert	X509Certificate2	Chứng thư số người ký. Được lấy từ AP hoặc MSSP từ số điện thoại của người ký. Trường chỉ đọc
TsaUrl	String	Địa chỉ máy chủ dịch vụ cấp dấu thời gian TSA
SignatureImage	System. Drawing. Image	Hình ảnh chữ ký
SignatureAppearance	PdfSignatureAppearance. RenderingMode	Chế độ hiển thị chữ ký: Hình ảnh (GRAPHIC); Hình ảnh và Thông tin (GRAPHIC_AND_DESCRIPTION); Thông tin (DESCRIPTION)
MSSPMode	Bool	- True: sử dụng dịch vụ MSSP để ký số trên SIM;

		- False: Sử dụng AP của BCYCP để test ký số SIM (Không cần thực hiện test trên máy có IP cố định đã đăng ký)
Phone	String	Số điện thoại SIM-PKI của người ký
MessageToBeDisplayed	String	Thông báo xác nhận ký số sẽ hiển thị trên điện thoại lắp SIM-PKI khi yêu cầu ký số được gửi tới điện thoại
SignerName	String	Họ tên người ký phê duyệt văn bản điện tử
APCertificate	String	Đường dẫn keystore đăng nhập MSSP do BCYCP cấp dạng file .p12
APCertPassword	String	Mật khẩu file p12
APID	String	Tên đăng nhập MSSP do BCYCP cấp
APPWD	String	Mật khẩu đăng nhập MSSP do BCYCP cấp
AllowOnlineCheckingCert	Bool	Kiểm tra trạng thái chứng thư số người ký trực tuyến
AllowCheckingCertViaOCSP	Bool	Kiểm tra chứng thư số người ký bằng dịch vụ OCSP
SignatureWidth	Int	Độ rộng chữ ký theo đơn vị Points (1px = 0.75pt)
SignatureHeight	Int	Độ cao chữ ký theo đơn vị Points

b. Các phương thức:

- *Contructor khởi tạo đối tượng: public PdfSigner(string inputPdf, string outputPdf, String phone, String signerName).*

Bao gồm các tham số:

+ inputPdf: Đường dẫn tệp PDF cần ký;

+ outputPdf: Đường dẫn lưu tệp PDF đã ký;

+ phone: Số điện thoại SIM-PKI của người ký;

+ signerName: Tên người ký văn bản phát hành

- *Hàm ký số tự động xác định vị trí chữ ký: public void SignApprove()*

Các lỗi phát sinh:

+ ArgumentException: Tham số ký không hợp lệ

+ GetCertException: Lỗi quá trình lấy chứng thư số từ MSSP hoặc AP

+ CertCheckingException: Lỗi quá trình kiểm tra chứng thư số

+ SignatureException: Lỗi ký số

+ Exception: Lỗi tiến trình

- *Hàm xem trước file ký: public void PreviewSignature()*

Với hàm này, các tham số cần thiết là đường dẫn tệp đầu vào, tên người ký văn bản, và hình ảnh chữ ký. Hàm sẽ trả về file PDF với hình ảnh chữ ký được gắn trên PDF để người dùng kiểm tra xem quá trình tự động xác định vị trí chữ ký có chính xác hay không? ***Do chỉ gắn hình ảnh chữ ký mà không có nội dung chữ ký nên khi kiểm tra chữ ký sẽ nhận được không báo lỗi định dạng chữ ký.***

Các lỗi phát sinh:

+ ArgumentException: Tham số ký không hợp lệ

+ SignatureException: Lỗi ký số

+ Exception: Lỗi tiến trình

- *Hàm ký số với tọa độ xác định trước: public void SignLoc(int iPage, int llx, int lly, int iWidth, int iHeight)*

Các tham số yêu cầu:

+ iPage: là trang đặt hiển thị chữ ký

+ llx: tọa độ X của điểm dưới bên trái (lower left X) của khung hiển thị chữ ký

+ lly: tọa độ Y của điểm dưới bên trái (lower left Y) của khung hiển thị chữ ký

+ iWidth: độ rộng khung hiển thị chữ ký

+ iHeight: độ cao khung hiển thị chữ ký

Các lỗi phát sinh:

+ ArgumentException: Tham số ký không hợp lệ

+ GetCertException: Lỗi quá trình lấy chứng thư số từ MSSP hoặc AP

+ CertCheckingException: Lỗi quá trình kiểm tra chứng thư số

+ SignatureException: Lỗi ký số

+ Exception: Lỗi tiến trình

- *Cặp hàm thực hiện ký số với mã xác thực (Validation Code – VC):*

+ Hàm tạo mã xác thực: public ValidationInfo CalculateVC()

Hàm này sẽ thực hiện tạo mã xác thực từ các tham số ký số: tệp đầu vào, hình ảnh chữ ký, chứng thư số người ký, thiết lập hiển thị chữ ký trên tài liệu PDF.

Lớp ValidationInfo bao gồm các thông tin sau:

```
public class ValidationInfo
 {
        //1. Chuỗi mã xác thực để hiển thị trên giao diện App di động
        public String ValicationCode { get; set; }
```

```
        //2. Tên trường chữ ký trên tài liệu PDF
        public String FieldName { get; set; }
        //3. Tên tệp PDF cần ký số
        public String FileName { get; set; }
        //4. Đường dẫn tệp tạm được sinh ra, dùng để đóng gói
        // chữ ký số ở hàm SignFinal
        public String TempFileName { get; set; }
        //5. Chứng thư số người ký
        public byte[] SignerCert { get; set; }
        //6. Mã băm của tài liệu PDF
        public byte[] Digest { get; set; }
        //7. Mã băm và thông tin thời gian ký
        public byte[] SecondDigest { get; set; }
}
```

Kết quả của hàm CalculateVC sẽ được sử dụng trong hàm SignFinal dưới đây. Ứng dụng di động sẽ lấy giá trị ValicationCode và hiển thị trên giao diện. Sau đó, AppService sẽ gọi hàm SignFinal, để gửi yêu cầu ký trên SIM, trên SIM sẽ tính toán lại giá trị ValidationCode và hiển thị trên màn hình xác nhận ký số. Khi đó người dùng có thể so sánh hai giá trị ValidationCode hiển thị trên giao diện app và trên thông báo xác nhận ký số để đảm bảo tính chính xác của giao dịch.

+ Hàm hoàn thành ký số: public void SignFinal(ValidationInfo vi)

Tham số hàm là kết quả được tính từ hàm CalculateVC. Hàm này sẽ gọi đến SIM để thực hiện ký số, trong quá trình đó, mã xác thực sẽ được hiển thị trên thông báo xác nhận ký số để người dùng kiểm tra.

3. Yêu cầu cần triển khai

- Máy chủ hệ điều hành Windows (có thể máy ảo) để cài đặt dịch vụ hỗ trợ ký số di động (AP – Application Provider). Trên máy chủ có cài đặt Web Server IIS. (Ví dụ: Windows Server 2012, IIS 8). Nếu hệ thống máy chủ QLVB hoặc máy chủ dịch vụ cho ứng dụng di động của đơn vị đang sử dụng Windows Server thì có thể sử dụng chung.

- Địa chỉ IP đầu ra cố định để máy chủ dịch vụ ký số di động trên có thể kết nối đến dịch vụ MSSP (Mobile Signature Service Provider) của Ban Cơ yếu Chính phủ.

- Tên miền (domain/subdomain) để cấp chứng thư số SSL cho dịch vụ hỗ trợ ký số.

4. Các bước triển khai tích hợp ký số trên di động sử dụng SIM-PKI

- Bước 1: Cung cấp địa chỉ IP đầu ra của máy chủ sẽ cài đặt dịch vụ hỗ trợ ký số di động (AP) để Ban Cơ yếu cấp thông tin truy cập vào dịch vụ MSSP bao gồm: apid và password.

- Bước 2: Lập danh sách yêu cầu đăng ký cấp chứng thư số SSL cho dịch vụ hỗ trợ ký số và chứng thư số để đăng nhập dịch vụ MSSP của BCY.

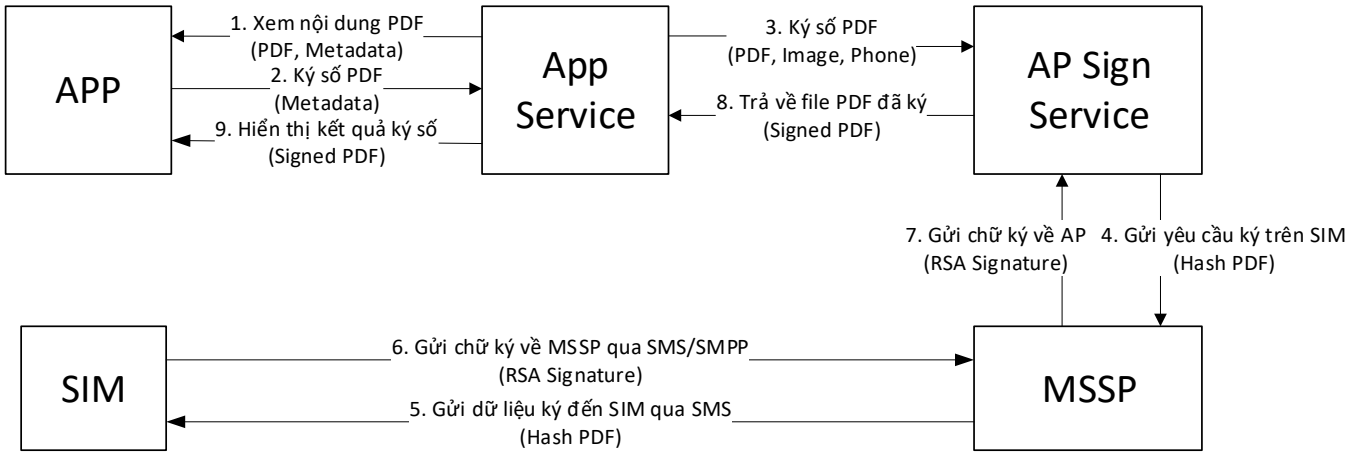
- Bước 3: Xây dựng Webservice trên .Net Framework 4.5 trở lên để tích hợp thư viện hỗ trợ ký số tệp PDF sử dụng SIM-PKI.

Trong trường hợp đơn vị chưa xây dựng xong WebService riêng, thì có thể sử dụng mẫu WebService dựng sẵn để kiểm thử giải pháp.

- Bước 4: Triển khai cài đặt WebService ký số lên máy chủ APP Server. Cấu hình SSL, với yêu cầu: Client Certificate đặt Require.

- Bước 5: Tích hợp WebService ký số vào App Service của ứng dụng đi động

5. Luồng dữ liệu ký số



- Bước 1: Người dùng mở giao diện App trên di động xem nội dung tệp PDF cần ký

- Bước 2: Người dùng thao tác ký số trên giao diện App, App sẽ gửi thông tin cần thiết về file PDF cần ký cho App Service.

- Bước 3: App Service lấy nội dung PDF cần ký, thông tin ảnh chữ ký của người ký, số điện thoại người ký và gọi API ký số trên AP Sign Service.

- Bước 4: AP Sign Service thực hiện băm nội dung tài liệu PDF cần ký số và gửi yêu cầu ký số đến SIM thông qua MSSP

- Bước 5: MSSP gửi yêu cầu ký số nhận được từ AP Sign Service đến SIM thông qua SMS với dữ liệu băm nội dung PDF.

- Bước 6: SIM thực hiện ký số và tra về giá trị chữ ký số RSA Signature cho MSSP thông qua SMS.

- Bước 7: MSSP trả về giá trị chữ ký số RSA Signature cho AP Sign Service để đóng gói theo định dạng PDF và lưu thành file PDF đã ký.

- Bước 8: AP Sign Service trả về file PDF đã ký cho App Service

- Bước 9: App Service thông báo kết quả, App hiển thị kết quả ký số cho người dùng.

6. Thiết lập máy chủ dịch vụ AP

6.1. Phần cứng máy chủ dịch vụ AP có thể theo lựa chọn sau:

Hệ điều hành	Windows Server 2012
CPU, RAM, Hard drive, etc	CPU: 1 x Intel® Xeon-Silver 4110 (2.1GHz/8-core/85W)
	Memory: 2 x 16 GB RDIMM DR 2600 MT/s (2 x 16 GB)
	Hard drive: Intel D3-S4510 960GB, SATA 6Gb/s, 3D, TLC 2.5", 7.0mm
	Network Controller: 1Gb Ethernet 2-Port 331i Adapter plus

6.2. Yêu cầu

- Yêu cầu phải có Static IP đầu ra cho máy chủ AP để cấp apid

- Yêu cầu domain để cấp chứng thư số cho webservice và chứng thư số cho AP kết nối MSSP.

6.3. Các bước cài đặt dịch vụ AP:

Bước 1: Cài đặt .net framework 3.5, 4.5. Yêu cầu: File cài đặt .Net 3.5

Bước 2: Cài đặt dịch vụ web server IIS. Chú ý Enable Client Certificate Mapping Authentication.

Bước 3: Cài đặt Webservice MPKISignService. Cấu hình license, AP certificate (p12), MSSP_MODE, APID và Password, Dịch vụ OCSP, CRL. Cấu hình SSL Client Authentication, Configuring IIS Mapping: Disable Anonymous Authentication.

Bước 4: Test ứng dụng kết nối đến dịch vụ.