Travaux pratiques 1 : PKI

Abdel-Malik FOFANA
Ivan KRIVOKUCA

1. Les différentes solutions de PKI :

0) Qu'est ce qu'une PKI :

Une PKI, ou infrastructure à clé publique, est un ensemble de technologies et de procédures qui permettent d'authentifier l'identité d'un utilisateur ou d'un appareil, et de chiffrer les données.

En termes simples, une PKI sait deux choses :

Qui est qui ? Grâce à l'authentification, une PKI permet de vérifier l'identité d'un utilisateur ou d'un appareil. Cela permet de s'assurer qu'on communique avec la personne ou l'appareil qu'on pense être.

Comment protéger les données ? Grâce au chiffrement, une PKI permet de rendre les données illisibles pour les personnes non autorisées. Cela permet de protéger les données contre le vol ou la modification.
La PKI est utilisée dans de nombreuses applications, notamment :

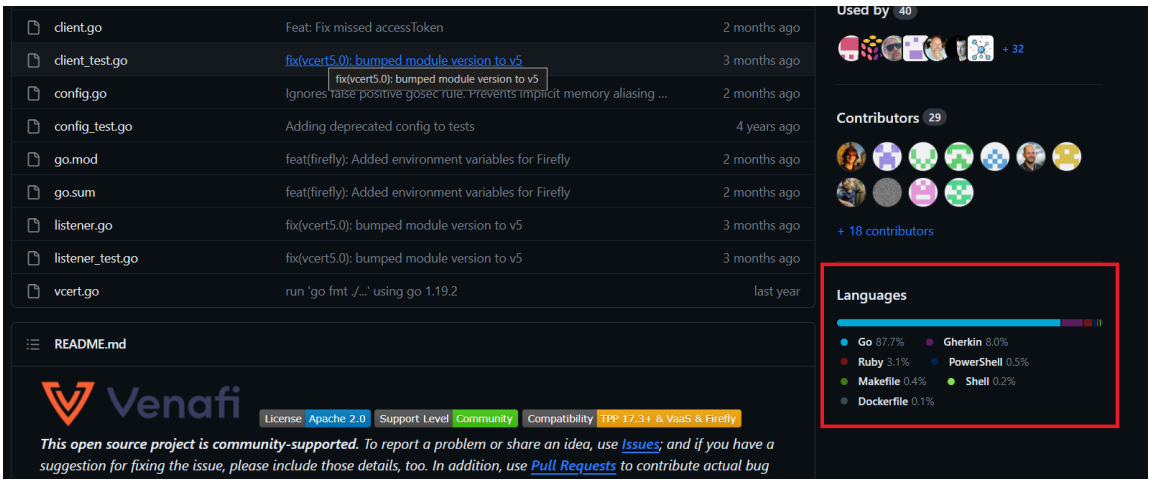
La connexion sécurisée à un site Web
L'envoi d'un e-mail sécurisé
La signature électronique d'un document
Le chiffrement des données sur un appareil mobile
1)PKI opensource:

2)PKI propriétaires :

Venafi: https://venafi.com/ (payant et une partie seulement du code est open source)

Les langages de programmation utilisés par Venafi sont Go, Java, Python, and Ruby :

https://marketplace.venafi.com/xchange/620d2d6ed419fb06a5c5bd36/solution/62bdf68ae5cbde2faa43fc62



Systèmes d'exploitation pris en charge :
https://docs.venafi.com/Docs/23.3PDF/Installation_Guide.pdf

à la page 27 on nous dit que windows , linux et macos sont suporté :

Server Agent

- Windows
  - .NET 4.7.2
  - Windows 8.1 or later
  - Windows Server 2012 R2 or later
- Linux versions tested by Venafi
  - Debian 8 and later
  - Ubuntu 16.04 and later
  - CentOS 7 and later
  - Red Hat Enterprise Linux (RHEL) 7 and later
  - May be compatible with other Linux distributions
- macOS
  - PKCS#11 and GPG: Yosemite 10.10 and later
  - Keychain integration: Catalina 10.15 and later

Microsoft PKI

La PKI (Public Key Infrastructure) de Microsoft est une solution de gestion de clés et de certificats numériques offerte par Microsoft. Elle permet de créer, de gérer et de distribuer des certificats numériques, ce qui est essentiel pour sécuriser les communications et les transactions électroniques. Voici quelques informations clés sur la PKI de Microsoft :

Windows Server : La PKI de Microsoft est principalement conçue pour fonctionner sur les serveurs Windows. Les versions prises en charge incluent Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, et

probablement des versions plus récentes à partir de ma dernière mise à jour en janvier 2022.
preuve :
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/windows-pki-documentation-reference/ba-p/1128393

Langages de programmation :
Pour interagir avec la PKI de Microsoft, vous pouvez utiliser divers langages de programmation, notamment :
PowerShell : Microsoft propose des modules PowerShell pour la gestion de la PKI.
C# : Vous pouvez également développer des applications personnalisées en utilisant des bibliothèques .NET pour travailler avec la PKI.
Liens Web :

Pour des informations officielles et des ressources sur la PKI de Microsoft, vous pouvez visiter le site Web de Microsoft dédié à la sécurité : https://www.microsoft.com/en-us/security
Pour des informations spécifiques sur la PKI, consultez la documentation technique de Microsoft, notamment les articles de la bibliothèque TechNet

(https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc771679(v=ws.11)).

2. Rechercher et lister les différentes Autorités de Certification (AC)

Il existe de nombreuses autorités de certification (AC) dans le monde. Elles peuvent être divisées en deux catégories principales : les AC publiques et les AC privées.

AC publiques

Les AC publiques sont des organisations qui émettent des certificats à des tiers, tels que des individus, des entreprises ou des organisations. Elles sont généralement gérées par des gouvernements ou des organismes de réglementation.

Voici quelques exemples d'AC publiques :

AC françaises : AC-Cert, Certeurope, OVHcloud, etc.
AC européennes : QuoVadis, GlobalSign, Comodo, etc.
AC américaines : DigiCert, Entrust, Symantec, etc.

AC privées

Les AC privées sont des organisations qui émettent des certificats à leurs propres utilisateurs ou clients. Elles sont généralement utilisées par les entreprises pour sécuriser leurs communications et leurs données.

Voici quelques exemples d'AC privées :

AC d'entreprise : Microsoft, Google, Apple, etc.
AC de fournisseur de services : Amazon Web Services, Microsoft Azure, etc.
AC de secteur : Fédération bancaire française, Chambre de commerce et d'industrie, etc.

bonus : on peut également trouvé une liste de toutes les ac europeennes sur le site ce site du gouvernement https://www.marches-publics.gouv.fr/agent/footer/info-acrgs

Le ministere de la justice (coucou) est une ac française par exemple

—----------

Une infrastructure à clés publiques (Public Key Infrastructure) est un ensemble de composants physiques, de procédures humaines et de logiciels destiné à gérer les clés publiques des utilisateurs d'un système. Elle permet d'authentifier les utilisateurs et les appareils, de chiffrer les données et de signer numériquement les documents.

Les principaux éléments d'une PKI comprennent :

- Les autorités de certification (CA)
- Les certificats numériques
- Les clés publiques et privées

On peut distinguer deux types d'implantation d'infrastructure PKI, celle qui utilisent les modèles Open Source et ceux qui utilisent des solutions propriétaires.

PKI Open Source

D'après *Guide des Solutions Libres Open Source* proposé par l'entreprise *Smile*, plusieurs possibilités sont proposées pour pouvoir utiliser l'implémentation PKI.

OpenSSL

Commencé en 1998, développé en C et disponible sur tous les systèmes d'exploitation actuelle, OpenSSL est une bibliothèque open source (Licence Apache version 2.0) largement utilisée pour la mise en œuvre de protocoles de sécurité. OpenSSL utilise la norme standard *X.509* (format standard pour certificats de clé publiques). Utilisé entant sous forme de ligne de commande.

Une documentation complète pour mettre en place mettre en une PKI sous OpenSSL est disponible ici : https://pki-tutorial.readthedocs.io/en/latest/. On remarque que OpenSSL permet la génération de clés, la création de CSR (Certificate Signing Request), la signature de certificats, la gestion de certificats, ainsi que la sécurisation des communications (en utilisant TLS/SSL) pour chiffrer les données et assurer l'authentification des entités.

OpenCA

Sous licence Apache et développé par OpenCA Labs, une organisation libre et communautaire qui a pour objectif de définir les standards d'un logiciel PKI démarrée dans les années 1999. Basé sous OpenSSL pour son moteur cryptographique et une interface web écrite en Perl/Javascript.

Brièvement, OpenCA permet de faire tout ce que OpenSSL permet déjà de faire mais avec un système de gestion de PKI complet qui fonctionne comme un serveur web (et ainsi une base de données, ce qui permet de pouvoir garder une trace des certificats signés/révoqués)

EJBCA

Basé sous Java et sorti en 2001, développé par l'entreprise suédoise PrimeKey Solutions sous licence LGPL. Le logiciel EJBCA est basé sur la librairie CESeCore, qui s'appuie elle-même sur l'api cryptographique Bouncy Castle.