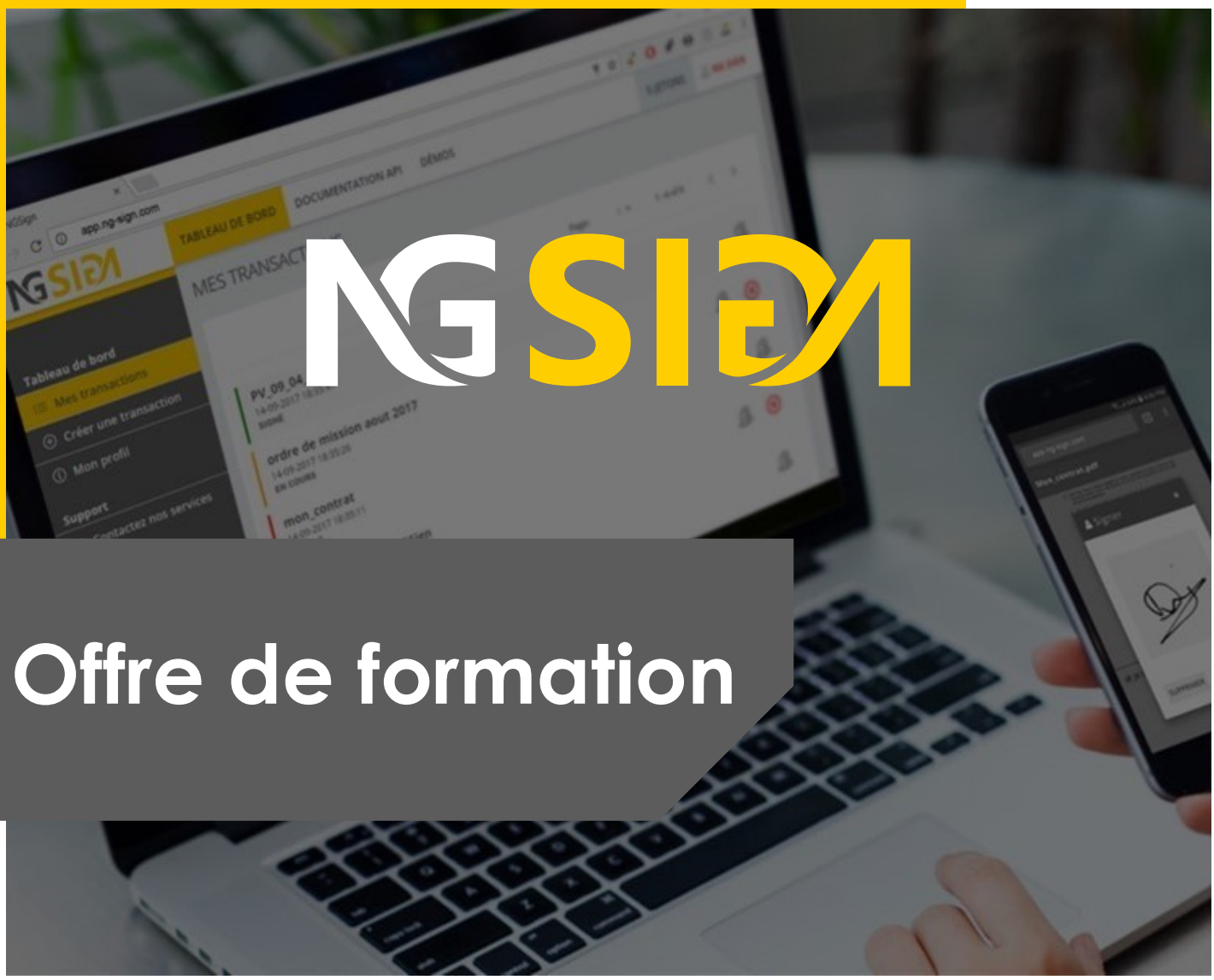


Offre de formation

PKI et Signature Électronique

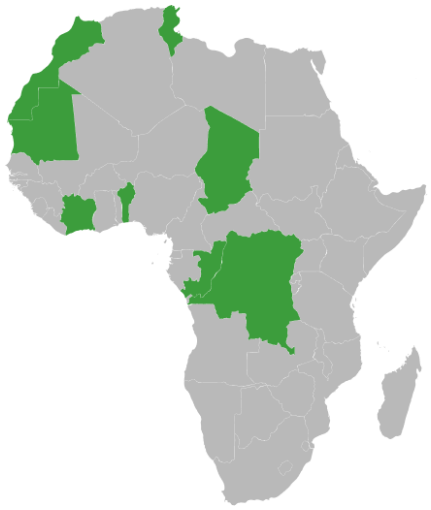
TABLE DES MATIÈRES

QUI SOMMES NOUS

L'expert de la confiance électronique

Fondée en 2016 par des experts en cryptographie et signature électronique (+ 20 ans), spécialiste de la signature électronique et les infrastructures à clé publique (PKI) et l'éditeur de la première plateforme web de signature électronique en Afrique.

3M+ Signature Électroniques	**2K+** Clients Cloud
15+ Projets eGov	**10+** Projets FinTech



Le premier acteur privé certifié eIDAS en Afrique.

NGSign est la premiere autorité de certification certifiée eIDAS Qualified Trust Service Provider en Afrique. Notre solution PKI a été également certifiée selon les normes ETSI EN 319 401, ETSI EN 319 411 et ETSI EN 319 412.

QSCert

We cover credibility

QSCert, spol. s r. o.
Certification body certifying products
E. P. Voljanskeho 1, 960 01 Zvolen, Slovak Republic

hereby grants the

CERTIFICATE

SNAS
Reg. No. 091/P-049

confirming, that the company

NG Technologies

NGSign, Immeuble les orangers, Rue Lac d'Annecy, Les Berges du Lac Etage 3, Tunis 1053

Provides qualified trusted services according to the Certification Scheme for eIDAS ver. 0.3 for the following services:

Qualified trust service for creation and validation of qualified certificates for electronic signature

Certified locations:: Immeuble les orangers, Rue Lac d'Annecy, Les Berges du Lac Etage 3, Tunis 1053, Tunisia

Based on the certification audit, protocol no. 10172/21 and surveillance audit, report No. 10172/21-2, it has been demonstrated that the trust services provided comply with the requirements of EU Regulation no. 910/2014 (eIDAS): Art. 5, Art. 8, Art. 11 par. 3, Art. 13, Art. 15, Art. 17 par. 5, Art. 19, Art. 21, Art. 22, Art. 23, Art. 24, Art. 26, Art. 27, Art. 28, Art. 29, Art. 31 and Annexes I and II and standards: ETSI EN 319 401 V2.2.1, ETSI EN 319 411-1 V1.2.2, ETSI EN 319 411-2 V2.2.2, ETSI EN 319 412-1 V1.4.1, ETSI EN 319 412-2 V2.2.1 a ETSI EN 319 412-5 V2.3.1.

Certificate No.:	eIDAS – 10172/21-1-2
Initial certification date:	24.08.2021
Date of issue:	17.12.2021
Expiry date:	23.08.2023

Trusted service policy:

- Certification Policy of the Root Certification Authority Remote Trust CA, version 1.0
- Certification Policy of the Intermeidate Certification Authority – Remote Trust CA version 1.0

By issuing this certificate, the validity of certificate P – 10172/21 of 24.08.2021 is cancelled.

CERTIFICATION BODY QSCert

This certificate is valid only if it is published among valid certificates on www.qscert.com

Ing. Marcel Šlúch
chief executive

FORMATION PKI ET SIGNATURE ELECTRONIQUE

Introduction

Dans un monde de plus en plus numérique et connecté, la sécurité des communications et des transactions en ligne est d'une importance cruciale. C'est là que la cryptographie et son application dans la PKI (Infrastructure à clé publique) jouent un rôle essentiel. Cette formation vise à vous familiariser avec les concepts fondamentaux de la cryptographie, la PKI et les services de confiance comme la signature électronique. Les deux principaux objectifs de cette formation sont de comprendre 1) comment une PKI permet de protéger et sécuriser efficacement les informations sensibles et les communications en ligne et 2) comment déployer une PKI en pratique.

• Au cours de cette formation

- Nous allons explorer les bases de la cryptographie et vous découvrirez comment ces techniques sont utilisées pour garantir la confidentialité, la non-répudiation, l'intégrité et l'authenticité des données, essentielles dans un monde où la protection des informations est une priorité.
- Nous plongerons également dans le fonctionnement de la PKI, un système complexe de gestion des clés publiques et privées. Vous apprendrez comment les certificats numériques sont émis, vérifiés et révoqués pour établir en toute confiance l'identité des parties prenantes lors des transactions électroniques.

- Au-delà des concepts théoriques, nous examinerons les applications concrètes de la cryptographie et de la PKI dans des domaines tels que les communications sécurisées, la signature électronique, l'authentification forte, le cachet électronique visible...

Objectif

Notre objectif est de vous fournir des compétences pratiques pour mettre en œuvre et gérer la sécurité basée sur la cryptographie et la PKI dans votre environnement professionnel. Vous serez en mesure de concevoir des solutions robustes pour protéger vos données et vos communications contre les menaces croissantes liées à la cybercriminalité.

A l'issue de la formation, les participants seront capables de :

- Avoir une compréhension globale des algorithmes cryptographiques mis en œuvre dans une PKI
- Avoir une compréhension globale des principaux acteurs d'une PKI : autorité de certification, autorité d'enregistrement, autorité d'horodatage...
- Avoir une compréhension globale des principaux services de confiance basés sur PKI
- Avoir une compréhension technique des supports cryptographiques (administration / développement) tels que les HSMs et les tokens PKCS#11 en général
- Être capable de générer des certificats d'autorité de certification ou d'entité finale à l'aide d'outils tels que openssl…
- Être capable d'effectuer différentes opérations de parsing, validation de différents objets signés d'une PKI (certificats, CRLs, OCSP...)
- Être capable de comprendre et de valider des documents signés…

Durée

4 jours de formation + 1 jour de visites.

Prérequis

- Bonne connaissance des systèmes, des réseaux et de la sécurité informatique.

Type

Théorique et pratique :

- Fourniture de supports pour les cours théoriques
- Mise à disposition des équipements pour les cours pratiques
- Attestations de formation nominatives
- Une journée détente et visite à notre infrastructure PKI dans un Data Center Tier 4 incluse

LES FORMATEURS

Dr. Moez Ben Mbarka

Docteur en informatique avec une thèse sur la signature électronique, Expert PKI et CEO de NGSIGN

- PhD in cryptography and electronic signatures with focus on long term validation of electronic signatures and techniques to renew cryptographic proofs.
- More than 15 years of experience in the implementation of PKI solutions and support for eIDAS and ETSI certifications
- Participated as an expert in ETSI working groups specializing in electronic signatures (ESI) Task Forces: ”Quick fixes to electronic signatures profiles”, ” Quick fixes to electronic signatures standards”, « Rationalised Framework for electronic signatures standards”, « Signature Creation and Validation and Trusted Service Providers (TSP) supporting eSignatures”
- Co-author of many ETSI standards:
    - ETSI TS 319 102 “Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation”
    - ETSI TS 103 173: Electronic signatures and infrastructures (ESI); CAdES baseline profile V2. 1.1
    - ETSI TS 103 174: Electronic signatures and infrastructures (ESI); ASiC baseline profile v2. 1.1
    - ETSI TS 103 172: Electronic signatures and infrastructures (ESI); PAdES baseline profile V2. 1.1
    - ETSI TS 102 853: Electronic signatures and infrastructures (ESI); signature validation procedures and policies v1. 1.1
    - ETSI TS 103 171: Electronic signatures and infrastructures (ESI); XAdES baseline profile V2. 1.1
- Managed many European research projects (2010-2015):
    - PAMPA (Password Authentication and Methods for Privacy and Anonymity)
    - TURBINE (TrUsted Revocable Biometric IdeNtitiEs)
    - SAVE (Sécurité et Audit du Vote Electronique)

Ing. Khadija Ferjani

Ingénieur en informatique, Experte en PKI et signature électronique et Directrice technique de NGSIGN

- Experience of more than 10 years in the development of PKI and electronic signature projects
- Experience of more than 10 years in the implementation of dematerialization and digital transformation solutions.
- Provided several PKI and electronic signature training sessions on behalf of public administrations and large accounts (banks, insurances…)
- 5 years of experience at Cryptolog (French TSP)
- Supervised the development of the Remote Trust PKI
- Supervised eIDAS/ETSI certifications of the PKI
- Supervised many security audits
- Certified ISO 27001 Lead Implementer;
- Certified nCipher nCSE (nCSE Examination Certificate)
- Certified Engineer – CryptoServer HSMs - UTIMACO HSM

PLAN DE FORMATION

Jour 1 - Introduction à la cryptographie et à la PKI

Concepts de base de la cryptographie : clés publiques et privées, chiffrement et hachage

Composants et acteur de la PKI : autorités et procédures

Certificat : le composant central de PKI - différents types de certificats et leurs utilisations

Type : Théorique

Jour 2 – Architecture PKI et usage

Gestion des certificats : cycle de vie des certificats

Architecture technique d'une PKI

Cérémonies des clés

Utilisation principale de PKI (services de confiance)

Type : Théorique

Jour 3 - Supports cryptographiques

Présentation des principaux dispositifs cryptographiques et keystores

Présentation de PKCS#11, Windows CAPI et Mac OS KeyChain

HSM (Hardware Security Module) – Administration et configuration

Développement avec HSM (génération de clé, cryptage, signature…)

Type : Théorique et pratique

Jour 4 – La PKI en pratique

Exemple de logiciel PKI : opensource, gratuit et commercial

Concevoir une PKI avec openssl :

Définition des profils de certificat

Génération des autorités de certification

Génération de certificats d'entité finale

Traiter avec CRL et OCSP

Validation d'un certificat

Signature électronique : Voir en détail les composants et la validation d'un document signé (à l'aide d'outils opensource)

Type de cours : Cours pratiques utilisant des ordinateurs et HSM.

CONDITIONS ET PRIX

Sessions	Session novembre : du 13 au 17 novembre 2023 Session février : du 19 au 23 février 2024
Nombre de places	Limité à un maximum de 12 personnes par session.
Prix / personne	2450 EUR - Hors Taxes.
Prix spécial groupes	10% de remise pour la deuxième personne 15% de remise à partir de la troisième personne.
Conditions de paiement	Paiement en avance au plus tard 2 semaines avant le début de la formation.
Ce qui est inclus dans le prix	Les supports de formation La visite au Datacenter PKI 2 diners de réseautages et d'échanges
Hébergement	Le nom et l'adresse de l'hôtel seront communiqués à la confirmation. Une offre spécifique d'hébergement sera proposée aux participants.

Inscription

Nous vous invitons à consulter ce lien pour vous inscrire https://www.ng-sign.com/formation/

L'expert de la confiance électronique

Nous vous souhaitons un apprentissage enrichissant et interactif au cours de cette formation sur la cryptographie et la PKI. Préparez-vous à plonger dans le monde fascinant de la cryptographie moderne et à acquérir des compétences essentielles pour sécuriser l'avenir numérique.

Moez Ben Mbarka, CEO NG TECHNOLOGIES