DOCAPOSTE Institute

Formation Communication Quantique et Cryptographie

Présentation

Cette formation avancée aborde la communication quantique et la cryptographie quantique sous l'angle de l'ingénierie, de la sécurité et du déploiement. Sur trois jours, les participants concevront des protocoles de distribution de clés (QKD), évalueront les modèles de menace et les preuves de sécurité, et optimiseront l'intégration avec les infrastructures classiques (réseaux, PKI, HSM).
Les TP s'appuient sur des simulateurs et des scénarios proches de la production pour produire des livrables auditables (paramétrage, métriques, rapports de risque).

Durée : 21,00 heures (3 jours)
Tarif INTRA : Nous consulter

Objectifs de la formation

- Concevoir une architecture de communication quantique intégrée à un SI (liens QKD, nœuds, orchestration, KMS)
- Optimiser et évaluer la sécurité de protocoles QKD (BB84/variantes), canaux, erreurs et fuites d'information
- Évaluer les modèles de menace, hypothèses et preuves de sécurité (information-theoretic, composabilité)
- Concevoir l'intégration crypto classique : usage des clés QKD (OTP, AES, TLS/IPsec), PKI et rotation
- Optimiser un plan de déploiement et d'exploitation (métriques, observabilité, SLA, conformité, gouvernance)
- Évaluer l'impact de la cryptographie post-quantique et définir une stratégie hybride PQC+QKD

Prérequis

- Maîtrise de la cryptographie classique : chiffrement symétrique/asymétrique, signatures, hachage
- Connaissances réseaux : TCP/IP, routage de base, TLS/IPsec, notions de latence/bande passante

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- Compréhension de la gestion de clés : PKI, rotation, stockage (HSM/keystore) et politiques d'accès
- Notions de probabilités/statistiques et d'algèbre linéaire (souhaitables)

Public

- Ingénieurs sécurité, architectes réseau, cryptographes applicatifs, responsables SSI, consultants et leads techniques intervenant sur des infrastructures critiques.
- Contextes : grands comptes, opérateurs, défense, finance, secteurs régulés, projets de modernisation crypto et exigences de souveraineté.
- Expérience attendue : maîtrise des bases de cryptographie classique, réseaux IP et principes de sécurité (PKI, TLS, gestion de clés).

Programme de la formation

Jour 1 – Fondations QKD et architecture de communication quantique

Session du matin :

- Architecture de communication quantique : lien quantique, canal classique authentifié, nœuds de confiance vs répéteurs (état de l'art)
- Protocoles QKD : BB84, bases, sifting, estimation d'erreur (QBER) et paramètres de session
- Chaîne de traitement : correction d'erreurs (EC) et amplification de confidentialité (PA) – rôle et coûts

Session de l'après-midi :

- Contraintes physiques et réseau : pertes, bruit, horloge/synchronisation, impact sur le key rate
- Gestion et distribution des clés : KMS, buffers, politiques de consommation et rotation
- Interfaçage SI : APIs, journalisation, traçabilité et séparation des responsabilités

TP / Exercice :

- Simuler une session BB84 sur canal bruité : générer qubits, exécuter sifting, calculer QBER, appliquer une correction d'erreurs simplifiée et une amplification

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

de confidentialité paramétrée. Livrable : notebook avec métriques (QBER, key rate, taux d'abandon) et recommandations de paramètres.

Points clés & takeaways :

- Concevoir une chaîne QKD de bout en bout et interpréter les métriques clés (QBER, key rate)
- Identifier les points de fragilité (pertes, bruit, synchronisation) et leurs impacts opérationnels
- Structurer l'intégration SI via un KMS et des politiques de consommation de clés

Jour 2 – Sécurité, preuves, attaques et stratégie hybride (QKD + PQC)

Session du matin :

- Hypothèses de sécurité : authentification du canal classique, confiance matériel, modèles de fuites
- Preuves et composabilité : notions de sécurité informationnelle, paramètres epsilon, marges et validation
- Attaques et contre-mesures : photon-number-splitting, attaques par canal auxiliaire, déni de service

Session de l'après-midi :

- Décoy states (initiation avancée) : principe, gains de sécurité, impacts sur le débit
- Cryptographie post-quantique : objectifs, intégration dans TLS et limites opérationnelles
- Stratégie hybride : scénarios d'usage, critères de choix, politique de transition et gestion des risques

TP / Exercice :

- Analyser un scénario d'attaque sur QKD (bruit induit, pertes ciblées, DoS) : détecter via métriques, ajuster seuils, documenter preuves et décisions d'arrêt/reprise. Construire une matrice de risques comparant PQC, QKD et hybride pour un cas d'usage (TLS/IPsec). Livrable : rapport de sécurité (constats, seuils, contre-mesures) + matrice de décision.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

Points clés & takeaways :

- Évaluer un modèle de menace QKD et relier hypothèses, preuves et paramètres de sécurité
- Identifier les attaques réalistes et définir des contre-mesures exploitables
- Définir une stratégie hybride PQC+QKD alignée sur le risque et l'opérabilité

Jour 3 – Intégration production : TLS/IPsec, exploitation, SLA et gouvernance

Session du matin :

- Intégration des clés QKD : modèles d'usage (OTP, AES), rotation, dérivation et séparation des clés
- Cas d'intégration : TLS/IPsec (surcouches), segmentation réseau, multi-sites et contraintes de latence
- Observabilité et exploitation : métriques (key rate, QBER, buffer), alerting, capacity planning

Session de l'après-midi :

- Résilience : gestion de panne de lien, bascule, dégradation contrôlée et politiques de continuité
- Conformité et gouvernance : traçabilité, audits, gestion des accès, exigences secteur régulé
- Industrialisation : runbooks, procédures de re-test, tests de charge et revue d'architecture

TP / Exercice :

- Intégrer un flux de clés QKD simulé dans un scénario de chiffrement applicatif : rotation, consommation, épuisement de buffer et bascule sur stratégie hybride. Construire un tableau de bord minimal (métriques + alertes) et un runbook d'exploitation. Livrable : configuration d'intégration + dashboard + runbook (SLA, seuils, procédures).

Points clés & takeaways :

- Concevoir une intégration QKD avec TLS/IPsec ou chiffrement applicatif en respectant la rotation
- Optimiser l'exploitation via métriques, alertes et runbooks orientés SLA

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- Mettre en place une gouvernance et une résilience adaptées aux contraintes de production

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Moyens pédagogiques et techniques

- Apports des connaissances communes.
- Mises en situation sur le thème de la formation et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.
- Equilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.
- Ressources documentaires en ligne et références mises à disposition par le formateur.
- Pour les formations en présentiel dans les locaux mis à disposition, les apprenants sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation :

- Recueil des besoins des apprenants afin de disposer des informations essentielles au bon déroulé de la formation (profil, niveau, attentes particulières...).
- Auto-positionnement des apprenants afin de mesurer le niveau de départ.

Tout au long de la formation :

- Évaluation continue des acquis avec des questions orales, des exercices, des QCM, des cas pratiques ou mises en situation...

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

A la fin de la formation :

- Auto-positionnement des apprenants afin de mesurer l'acquisition des compétences.
- Evaluation par le formateur des compétences acquises par les apprenants.
- Questionnaire de satisfaction à chaud afin de recueillir la satisfaction des apprenants à l'issue de la formation.
- Questionnaire de satisfaction à froid afin d'évaluer les apports ancrés de la formation et leurs mises en application au quotidien.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France