IEC 62541-2

Edition 1.0 2026-02

NORME INTERNATIONALE

Architecture unifiée OPC -
Partie 2: Modèle de sécurité

ICS 25.040

ISBN 978-2-8327-1035-7

IEC 62541-2:2026-02(fr)

IEC Secretariat
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, …). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications, symboles graphiques et le glossaire. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 500 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 25 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

Architecture unifiée OPC - Partie 2: Modèle de sécurité

AVANT-PROPOS

1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'IEC attire l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'IEC ne prend pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de brevet revendiqué à cet égard. À la date de publication du présent document, l'IEC n'avait pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse https://patents.iec.ch. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié tout ou partie de tels droits de brevet.

L'IEC 62541-2 a été établie par le sous-comité 65E: Les dispositifs et leur intégration dans les systèmes de l'entreprise, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels. Il s'agit d'une Norme internationale.

Cette édition annule et remplace la troisième édition de l'IEC TR 62541-2 parue en 2020. Cette édition constitue une révision technique.

Le texte de cette Norme internationale est issu des documents suivants:

Projet	Rapport de vote
65E/1201/FDIS	65E/1206/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/publications.

Dans l'ensemble du présent document et dans les autres parties de la série, certaines conventions de document sont utilisées:

Le format *italique* est utilisé pour mettre en évidence un terme défini ou une définition qui apparaît à l'article "Termes et définitions" dans l'une des parties de la série.

Le format *italique* est également utilisé pour mettre en évidence le nom d'un paramètre d'entrée ou de sortie de service, ou le nom d'une structure ou d'un élément de structure habituellement défini dans les tableaux.

Par ailleurs, les *termes* et les *noms en italique* sont souvent écrits en camel-case (pratique qui consiste à joindre, sans espace, les éléments des mots ou expressions composés, la première lettre de chaque élément étant en majuscule). Par exemple, le terme défini est *AddressSpace* et non Espace d'Adressage. Cela permet de mieux comprendre qu'il existe une définition unique pour *AddressSpace*, et non deux définitions distinctes pour Espace et pour Adressage.

Une liste de toutes les parties de la série IEC 62541, publiées sous le titre général *Architecture unifiée OPC*, se trouve sur le site web de l'IEC.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. À cette date, le document sera

– reconduit,
– supprimé, ou
– révisé.

1 Domaine d'application

La présente partie de l'IEC 62541 décrit le modèle de sécurité de l'Architecture unifiée OPC (OPC UA). Elle décrit les menaces pour la sécurité des environnements physiques, matériels et logiciels dans lesquels l'OPC UA est destinée à fonctionner. Elle décrit de quelle manière l'OPC UA s'appuie sur d'autres normes de sécurité. Elle fournit une définition des termes de sécurité communs utilisés dans la présente partie et dans les autres parties de la série IEC 62541. Elle donne une vue d'ensemble des fonctions de sécurité spécifiées dans d'autres parties de la série et en décrit le concept. Elle fait référence aux services, mappings et *Profils* spécifiés de manière normative dans d'autres parties de la série IEC 62541. Elle fournit des suggestions ou des lignes directrices sur les meilleures pratiques relatives à la mise en œuvre de la sécurité. Aucune ambiguïté apparente entre le présent document et l'une des autres parties normatives ne supprime ni ne réduit l'exigence spécifiée dans l'autre partie normative.

Il existe de nombreux aspects différents de la sécurité qui sont traités lors du développement d'applications. Cependant, étant donné que l'OPC UA spécifie un protocole de communication, l'attention est portée sur la sécurisation des données échangées entre les applications. Cela ne signifie pas qu'un développeur d'applications peut ignorer les autres aspects de la sécurité, comme la protection des données persistantes contre toute falsification. Il est important que les développeurs examinent tous les aspects de la sécurité et décident de la manière dont ces aspects peuvent être traités dans l'application. Les fonctions de sécurité communes pour les commandes industrielles sont définies dans l'IEC 62443-4-2; elles sont mises en corrélation avec l'OPC UA à l'Annexe A.

Le présent document s'adresse aux lecteurs qui développeront des applications OPC UA. Il s'applique également aux utilisateurs finaux qui souhaitent comprendre les différentes fonctions de sécurité fournies par l'OPC UA. Il fournit, par ailleurs, certaines recommandations qui peuvent être appliquées lors du déploiement de systèmes. Ces recommandations sont génériques par nature, car les détails dépendent de la mise en œuvre réelle des applications *OPC UA* et des choix effectués pour la sécurité du site.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 62541-1, *Architecture unifiée OPC - Partie 1: Vue d'ensemble et concepts*

3 Termes, définitions, abréviations et conventions

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'IEC 62541-1 ainsi que les suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

– IEC Electropedia: disponible à l'adresse https://www.electropedia.org/

– ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

3.1.1
AccessRestriction
limite sur les circonstances dans lesquelles une opération, telle qu'une lecture, une écriture ou un appel, peut être exécutée sur un *Nœud*

Note 1 à l'article: Des opérations ne peuvent être réalisées sur un *Nœud* que si le *Client* possède les *Permissions* nécessaires et satisfait à toutes les *AccessRestrictions*.

3.1.2
AccessToken
document signé numériquement qui certifie que le sujet a le droit d'accéder à une *Ressource*

Note 1 à l'article: Le document inclut le nom du sujet et de la *Ressource* à laquelle il accède.

3.1.3
ApplicationInstance
installation individuelle d'un programme exécuté sur un ordinateur donné

Note 1 à l'article: Il peut y avoir plusieurs *ApplicationInstances* de la même application qui s'exécute simultanément sur plusieurs ordinateurs ou, éventuellement, sur le même ordinateur.

3.1.4
ApplicationInstanceCertificate
Certificat d'une *ApplicationInstance* donnée qui a été installée sur un hôte donné

Note 1 à l'article: Des installations différentes du même produit logiciel ont des *ApplicationInstanceCertificates* différents. L'emploi d'un *ApplicationInstanceCertificate* pour des utilisations autres que celles décrites dans la présente spécification peut sensiblement réduire la sécurité fournie par l'*ApplicationInstanceCertificate* et il convient donc de l'éviter.

Note 2 à l'article: Également écrit sous la forme *Certificat ApplicationInstance*.

3.1.5
Cryptographie asymétrique

méthode de *Cryptographie* qui utilise une paire de clés, dont l'une est désignée *Clé privée* et gardée secrète, et l'autre, appelée *Clé publique*, est disponible au public

Note 1 à l'article: La Cryptographie asymétrique est également appelée "cryptographie à clé publique". Dans un algorithme de Chiffrement asymétrique, lorsqu'une entité "A" exige une *Confidentialité* des données envoyées à l'entité "B", l'entité "A" chiffre alors les données à l'aide d'une Clé publique fournie par l'entité "B". Seule l'entité "B" possède la Clé privée correspondante nécessaire pour déchiffrer les données. Dans un algorithme de Signature numérique asymétrique, lorsqu'une entité "A" exige l'Intégrité du message ou exige de fournir une *Authentification* pour les données envoyées à l'entité "B", l'entité A utilise sa Clé privée pour signer les données. Pour vérifier la signature, l'entité B utilise la Clé publique correspondante fournie par l'entité A. Dans un algorithme d'accord de clé asymétrique, l'entité A et l'entité B envoient chacune leur propre Clé publique à l'autre entité. Chacune utilise alors sa propre Clé privée et la Clé publique de l'autre entité pour calculer la nouvelle valeur de clé, conformément à l'IS Glossary.

3.1.6
Chiffrement asymétrique
mécanisme utilisé par la *Cryptographie asymétrique* pour chiffrer des données avec la *Clé publique* d'une entité et pour déchiffrer des données avec la *Clé privée* associée

3.1.7
Signature asymétrique
mécanisme utilisé par la *Cryptographie asymétrique* pour signer des données avec la *Clé privée* d'une entité et pour vérifier la signature des données à l'aide de la *Clé publique* associée

3.1.8
Vérifiabilité
objectif de sécurité qui assure que toute action ou toute activité d'un système peut être enregistrée

3.1.9
Audit
suivi des actions et des activités dans le système, y compris les activités relatives à la sécurité, où des enregistrements d'*Audit* peuvent être utilisés pour examiner et vérifier les opérations du système

3.1.10
Authentification
processus qui assure que l'identité d'une entité telle qu'un *Client*, un *Serveur*, un *Éditeur* ou un utilisateur peut être vérifiée

3.1.11
Autorisation
capacité à accorder l'accès à une ressource système

Note 1 à l'article: Il convient que l'*Autorisation* d'accès aux ressources soit fondée sur le principe du "besoin d'en connaître". Il est important que l'accès soit limité dans un système.

3.1.12
AuthorizationService
Serveur qui valide une demande d'accès à une *Ressource* et retourne un *AccessToken* qui donne accès à la *Ressource*

Note 1 à l'article: L'*AuthorizationService* est également appelé STS (*Security Token Service*, service de jeton de sécurité) dans d'autres normes.

3.1.13
Disponibilité
objectif de sécurité qui assure que le système fonctionne normalement. Autrement dit, aucun service n'a été compromis au point de devenir indisponible ou gravement dégradé

3.1.14
Autorité de certification
entité qui peut émettre des *Certificat*s, également connue sous le nom de CA

Note 1 à l'article: Le *Certificat* certifie la propriété d'une *Clé publique* par le sujet nommé du *Certificat*. Cela permet à des tiers (des parties dépendantes) de s'appuyer sur des signatures ou des assertions faites par la *Clé privée* qui correspond à la *Clé publique* certifiée. Dans ce modèle de relation de confiance, une CA est un tiers de confiance qui est à la fois le sujet (propriétaire) du *Certificat* et la partie qui dépend du *Certificat*. Les CA sont caractéristiques de nombreux schémas d'*Infrastructure à clés publiques* (PKI, *Public Key Infrastructure*).

Note 2 à l'article: Un système de CA privée (ou une sous-CA privée) peut être utilisé, sous réserve que toutes les parties lui fassent confiance.

3.1.15
CertificateStore
lieu persistant où sont stockées les *Certificats* et les listes de révocation de *Certificats* (CRL)

Note 1 à l'article: Il peut s'agir d'une structure de fichier résidant sur un disque ou, dans le cas de plateformes Windows, d'un emplacement du Registre Windows.

3.1.16
Revendication
déclaration dans un *AccessToken* qui atteste d'informations concernant le sujet dont le *Service d'autorisation* sait qu'elles sont vraies

Note 1 à l'article: Les *Revendications* peuvent inclure le nom d'utilisateur, l'adresse e-mail et les *Rôles* attribués au sujet.

3.1.17
Confidentialité
objectif de sécurité qui assure la protection des données contre la lecture par des parties auxquelles elles ne sont pas destinées

3.1.18
Cryptographie
algorithme qui transforme une information claire et significative en une forme chiffrée et inintelligible à l'aide d'un algorithme et d'une clé

3.1.19
Système de gestion de la cybersécurité
programme conçu par une organisation dans le but de maintenir la sécurité des actifs de l'ensemble de l'organisation à un niveau établi de *Confidentialité*, d'*Intégrité* et de *Disponibilité*, qu'ils concernent la partie commerciale ou la partie systèmes d'automatisation industrielle et de commande de l'organisation

3.1.20
Signature numérique
valeur calculée à l'aide d'un algorithme cryptographique et ajoutée aux données de sorte que tout destinataire des données puisse utiliser la signature pour vérifier l'origine et l'*Intégrité* des données

3.1.21
Intégrité
objectif de sécurité qui assure que les informations n'ont pas été modifiées ou détruites de manière non autorisée

Note 1 à l'article: Plus d'informations peuvent être obtenues en consultant l'IS Glossary.

3.1.22
Fournisseur d'identité
Serveur qui vérifie les authentifiants fournis par un *Principal de sécurité* et qui retourne un jeton pouvant être transmis à un *Service d'autorisation* associé

3.1.23
Algorithme d'échange de clés
protocole utilisé pour établir un chemin de communication sécurisé entre deux entités dans un environnement non sécurisé, par lequel les deux entités appliquent un algorithme spécifique pour échanger en toute sécurité des clés secrètes utilisées pour sécuriser la communication entre elles

Note 1 à l'article: Le protocole Handshake spécifié dans TLS est un exemple type d'*Algorithme d'échange de clés*.

3.1.24
Signature de message
Signature numérique utilisée pour assurer l'*Intégrité* des *Message*s qui sont envoyés entre deux entités

Note 1 à l'article: Il existe plusieurs manières de générer et de vérifier les *Signatures de message*, mais elles peuvent être classées en deux catégories: les approches symétriques (voir 3.1.35) et les approches asymétriques (voir 3.1.5).

3.1.25
Non-répudiation
aptitude à démontrer l'occurrence d'un événement ou d'une action revendiqué(e) et ses entités d'origine

Note 1 à l'article: La non-répudiation a pour objet de résoudre les litiges quant à la survenue ou pas de l'événement ou de l'action et à l'implication des entités dans l'événement.

Note 2 à l'article: Cette définition est issue de l'IEC 62443-4-2 et peut être différente de la définition utilisée dans d'autres secteurs.

3.1.26
Nonce
nombre aléatoire qui est utilisé une fois, généralement par des algorithmes qui génèrent des clés de sécurité

3.1.27
Permission
droit d'exécuter une opération, par exemple une lecture, une écriture ou un appel, sur un *Nœud*

3.1.28
Clé privée
composante secrète d'une paire de clés cryptographiques utilisée pour la *Cryptographie asymétrique*

Note 1 à l'article: La *Clé publique* et la *Clé privée* sont toujours générées sous la forme d'une paire. Si l'une d'elles est mise à jour, l'autre l'est également.

3.1.29
Clé publique
composante divulguée publiquement d'une paire de clés cryptographiques utilisée pour la *Cryptographie asymétrique*

Note 1 à l'article: Voir l'IS Glossary.

Note 2 à l'article: La *Clé publique* et la *Clé privée* sont toujours générées sous la forme d'une paire. Si l'une d'elles est mise à jour, l'autre doit également l'être.

3.1.30
Infrastructure à clés publiques
ensemble de matériels, logiciels, personnes, politiques et procédures nécessaires pour créer, gérer, stocker, distribuer et révoquer des *Certificats* fondés sur une *Cryptographie asymétrique*

Note 1 à l'article: Les principales fonctions d'ICP consistent à enregistrer les utilisateurs et à délivrer leurs *Certificats* à clé publique, à révoquer les *Certificats* si nécessaire et à archiver les données nécessaires pour valider les *Certificats*. Les paires de clés pour la *Confidentialité* des données peuvent être générées par une *Autorité de certification* (CA), mais il est préférable que le propriétaire de la *Clé privée* génère la paire de clés en local, sous réserve qu'il possède une fonctionnalité de génération de clés de confiance, car cela améliore la sécurité du fait que la *Clé privée* n'est jamais transmise à la CA. Voir ICP et X.509v3 pour plus d'informations sur les *Infrastructures à clés publiques*.

3.1.31
Ressource
entité sécurisée à laquelle une application accède

Note 1 à l'article: Une *Ressource* est généralement un *Serveur*.

3.1.32
Rôle
fonction assumée par un *Client* lorsqu'il accède à un *Serveur*

Note 1 à l'article: Un *Rôle* peut faire référence à une fonction professionnelle spécifique, telle qu'un opérateur ou un ingénieur.

3.1.33
SecurityKeyService
Serveur qui accepte des *AccessTokens* émis par le *Service d'autorisation* et qui retourne des clés de sécurité pouvant être utilisées pour accéder à la *Ressource* spécifiée.

Note 1 à l'article: Les clés sont généralement utilisées pour les opérations de cryptographie telles que le chiffrement ou le déchiffrement de messages envoyés sur un flux *PubSub*.

3.1.34
Canal sécurisé
dans l'OPC UA, chemin de communication établi entre un *Client* et un *Serveur* OPC UA qui se sont authentifiés en utilisant certains services OPC UA et pour lesquels des paramètres de sécurité ont été négociés et appliqués

3.1.35
Cryptographie symétrique
branche de cryptographie impliquant des algorithmes qui utilisent la même clé pour deux étapes différentes de l'algorithme (comme le chiffrement et le déchiffrement, ou la création de signature et la vérification de signature)

Note 1 à l'article: Voir l'IS Glossary.

3.1.36
Chiffrement symétrique
mécanisme utilisé par la *Cryptographie symétrique* pour le chiffrement et le déchiffrement de données avec une clé cryptographique partagée par deux entités

3.1.37
SecurityGroup
Éditeur(s) et *Abonné(s)* qui utilisent un contexte de sécurité partagé

Note 1 à l'article: Ce contexte peut inclure des clés de partage.

3.1.38
Signature symétrique
mécanisme utilisé par la *Cryptographie symétrique* pour la signature de données avec une clé cryptographique partagée par deux entités

Note 1 à l'article: La signature est ensuite validée en générant à nouveau la signature des données et en comparant ces deux signatures. Si elles sont identiques, la signature est alors valide; sinon, la clé ou les données sont différentes des deux entités.

3.1.39
TrustList
liste des *Certificats* auxquels une Application OPC UA, par sa configuration, fait confiance

3.1.40
Transport Layer Security
protocole normalisé pour la création de *Canaux sécurisés* sur des réseaux IP

3.1.41
Certificat X.509
Certificat dans l'un des formats définis par X.509 version 1, 2 ou 3

Note 1 à l'article: Un *Certificat X.509* contient une séquence d'éléments de données et comporte une *Signature numérique* calculée sur cette séquence. L'OPC UA utilise uniquement la V3.

3.2 Abréviations

AES (Advanced Encryption Standard)	Protocole AES
CA (Certificate Authority)	Autorité de certification
CRL (Certificate Revocation List)	Liste de révocation de certificat
CSMS (Cyber Security Management System)	Système de gestion de la cybersécurité
DNS (Domain Name System)	Système de noms de domaine
DSA (Digital Signature Algorithm)	Algorithme de signature numérique
ECDH (Elliptic Curve Diffie-Hellman)	Algorithme Diffie-Hellman fondé sur les courbes elliptiques
ECDSA (Elliptic Curve Digital Signature Algorithm)	Algorithme de signature numérique fondé sur les courbes elliptiques
GDS (Global Discovery Server)	Serveur de découverte global
HMAC (Hash-based Message Authentication Code)	Code d'authentification de message fondé sur un hachage
JSON (JavaScript Object Notation)	Notation objet issue de JavaScript
JWT (JSON Web Token)	Jeton Web JSON
NIST (National Institute of Standard and Technology)	Institut national des normes et de la technologie
PKI (Public Key Infrastructure)	Infrastructure à clés publiques
RSA (Rivest-Shamir-Adleman)	Algorithme de clé publique pour la signature ou le chiffrement
SHA (Secure Hash Algorithm)	Algorithme de hachage sécurisé (il en existe plusieurs versions, SHA1, SHA256, etc.)
SKS (Security Key Server)	Serveur de clés de sécurité
SSL (Secure Sockets Layer)	Protocole SSL
TLS (Transport Layer Security)	Protocole TLS
TPM (Trusted Platform Module)	Module de plateforme de confiance
UA (Unified Architecture)	Architecture unifiée
UACP (Unified Architecture Connection Protocol)	Protocole de connexion de l'Architecture unifiée
UADP (Unified Architecture Datagram Protocol)	Protocole datagramme de l'Architecture unifiée
URI (Uniform Resource Identifier)	Identificateur uniforme de ressources
XML (Extensible Mark-up Language)	Langage de balisage étendu

3.3 Conventions pour les figures du modèle de sécurité

Les figures du présent document n'utilisent aucune convention particulière. Toutes les conventions utilisées dans une figure particulière sont expliquées pour la figure en question.

4 Architecture de sécurité OPC UA

4.1 Environnement de sécurité OPC UA

L'OPC UA est un protocole utilisé entre les composants impliqués dans l'exploitation d'une installation industrielle à plusieurs niveaux: de la gestion d'entreprise de haut niveau à la commande directe de processus de bas niveau d'un appareil. L'utilisation de l'OPC UA pour la gestion d'entreprise implique des relations avec les clients et les fournisseurs. Elle peut constituer une cible attractive pour l'espionnage ou le sabotage industriel, et peut également être exposée à des menaces par l'intermédiaire de logiciels malveillants non ciblés tels que des vers circulant sur des réseaux publics. Une interruption des communications au niveau de la commande de processus peut engendrer des pertes financières, compromettre la sécurité des employés et la sécurité publique, voire occasionner des dégâts environnementaux.

L'OPC UA est destinée à être déployée dans différents environnements d'exploitation, caractérisés par différentes hypothèses en ce qui concerne les menaces et l'accessibilité, ainsi que par une diversité de politiques de sécurité et de régimes d'application de la loi. L'OPC UA fournit donc un ensemble souple de mécanismes de sécurité. La Figure 1 représente une combinaison de ces environnements. Certaines *Applications* OPC UA se trouvent sur le même hôte et peuvent facilement être protégées des attaques externes. Certaines *Applications* OPC UA se trouvent sur différents hôtes dans le même réseau d'exploitation et peuvent être protégées par les protections périphériques de sécurité qui séparent le réseau d'exploitation des connexions externes. Certaines *Applications* OPC UA sont exécutées dans des environnements relativement ouverts, où les utilisateurs et les applications peuvent être difficiles à contrôler. D'autres *Applications* OPC UA sont intégrées dans des systèmes de commande qui n'ont pas de connexion électronique directe avec des systèmes externes. L'OPC UA prend également en charge plusieurs protocoles et technologies de communication, qui peuvent exiger différents niveaux de sécurité et différentes infrastructures de sécurité. Par exemple, la communication Client - Serveur et Éditeur - Abonné est représentée à la Figure 1. L'OPC UA définit également des services globaux tels que la gestion des *Certificats*, la gestion des *KeyCredentials*, l'*AuthorizationService* et le *GlobalDiscoveryServer* (GDS) pour faciliter la gestion des fonctionnalités de sécurité et d'autres fonctionnalités globales.