Table des matières

AXIS-CSRM 7 : Le modèle de SECURITE 1
Introduction aux concepts 1
Concepts & Mécanismes 1
L'approche AXIS-CSRM et la sécurité : 3
Le spatial et le temporel : 4
Les intentions de sécurité Security intentions 4
La normalisation : 4
Sécurité intrinsèque et procédurale : 4
1.1.1.1 L'usage personnel / la communication à d'autres : 4
Primitives conceptuelles : 5
Authenticité : 5
Unicité : 6
Vie privée (Privacy) : 6
Qualités : 6
Communication & Combinaisons (AXE) : 7
Documents (Méta-Documents – Certificats – Documents signés – Conventions) 8
Méta-documents 8
Certificats : 8
Documents signés : 8
Conventions : 8

AXIS-CSRM 06 : Le modèle de SECURITE

AXIS-CSRM dans le modèle de sécurité se concentre sur l'enregistrement des agents, de leurs mandats et sur l'assurance de leur authenticité lorsqu'ils agissent.

Il couvre aussi l'assurance de l'intégrité des interactions entre les agents et de l'intégrité de l'exécution conformément à la consigne (le processus fait-il bien ce qu'il est censé faire et ne fait-il que cela ?). De même, pour l'intégrité et l'authenticité des AXEs ou de leurs composants.

Introduction aux concepts

Concepts & Mécanismes

La construction de la **confiance**; jusqu'à quel point peut-on se fier aux **données** pour construire l'**information** ? Le modèle de sécurité ou le modèle de la construction de la confiance. En fait le mot ''sécurité'' a un aspect protecteur, tandis que ''confiance'' traduit la construction de quelque chose de positif; l'objectif est de pouvoir se fier aux données pour construire l'information.

Ici trois mots sont importants :

- **confiance** : pouvoir se fier à quelque chose jusqu'à un certain point
- **données** : la façon par laquelle les informations sont représentées dans l'informatique
- **l'information** : construite au départ de la perception des données et qui constituent la référence pour les humains

Le modèle Conceptual Semantic Reference Model est tenu d'aborder certains aspects en vue de combiner les mécanismes et les concepts pour obtenir un certain nombre de propriétés. Il existe par exemple des primitives conceptuelles qui produisent des résultats liés à la confiance

Primitives conceptuelles : les principales primitives conceptuelles sont : Intégrité/Authenticité/ Unicité/Privacy/ Qualités diverses/ …

- La première et peut-être la plus importante c'est l'intégrité. La question est de savoir si les données publiées le sont de façon intègre, c'est-à-dire qu'elles n'ont pas été déformées lors de copies, ou à cause de supports impliqués.
- l'authenticité est la confiance placée par une personne dans l'identité d'un objet ou dans la déclaration d'identité d'une autre personne.
- l'unicité est la confiance dans le fait que l'objet ou la personne est vraiment unique. C'est relativement trivial pour des personnes physiques; c'est moins le cas pour une personne morale. Dans ce cas, il faut s'assurer qu'il n'y a pas deux personnes morales ayant la même identité. Il existe aussi des exemples d'usurpations d'identité voulues ou d'identifications de personnes réalisées de manière identique.
- la capacité de protection de la vie privée (privacy)

Force des mécanismes et dispositifs existants (la division par 97 ou corrections sophistiquées des erreurs pour le CD-Audio[i])

En fait il n'existe aucun système qui garantisse une sécurité, la confiance absolue. Dans ce cadre, il est nécessaire de mettre en place des mécanismes et des dispositifs qui procurent une confiance raisonnable, proportionnée au(x) danger(s) encourus. En termes techniques, la force des mécanismes et des dispositifs mis en œuvre[1].

- RSA / PGP / Courbes elliptiques / ZK RSA / PGP / Elliptic curves / ZK

Voici d'autres exemples plus complexes issus de systèmes de cryptographie. Le système RSA (Revest, Shamir & Adleman) a intrinsèquement des propriétés extrêmement solides. Un système comme le PGP (Pretty Good Privacy) possède d'autres types de propriétés qui suffisent dans bien des cas pour beaucoup d'applications. Certains systèmes de cryptographie sont basés sur des courbes elliptiques, ou un concept astucieux comme le Zero Knowledge (authentification de l'identité entre deux personnes avec apport de connaissance nulle pour celui qui intercepterait le dialogue entre ces deux personnes).

- Nombre efficace de bits des clés /

Le choix du nombre efficace de bits, des clés, … constituent un autre élément important. Il est évident que plus il y a de bits, plus la sécurité est forte … théoriquement. A la condition expresse qu'il n'existe aucun trucage. Dans certains cas, le système est réputé avoir 1024 bits/clé, alors qu'en réalité il embarque une réduction efficace (BRR : Bit Rate Reduction) Ce sont des clés dites ''entropiques'' qui peuvent être la conséquence d'un abus de pouvoir d'un des acteurs.

- Cartes à puces / TRD Smart Cards / TRD

Au niveau des dispositifs, la carte à puce a fait ses preuves comme étant un système avec des informations embarquées et une capacité de calcul. Dans ces cas-là le système procure une protection relativement sérieuse de la connaissance des clés mais aussi d'autres types d'informations. Toute une série de problèmes

[1] Exemple : Dans le numéro de compte d'un client d'une banque belge, le code de vérification est simplement le reste de la division par 97 des nombres précédents. C'est une manière de s'assurer que les numéros des comptes bancaires sont valides, mais pas que le numéro de compte corresponde au titulaire. La RTBF avait adopté le même dispositif pour la numérotation des bandes magnétiques 1 pouce et Betacam.

cryptographiques ont été résolus par des agencements de primitives conceptuelles protégées, assemblées ou organisées au sein de la carte.

Le TRD (Tamper-Resistant Device) est une espèce de coffre-fort avec des moyens de traitement de données. Ces dispositifs sont conçus pour traiter ou garder des informations. Dès la fermeture, plus personne ne peut accéder à l'information du TRD, même pas ceux qui l'ont conçu et fermé. Cette technologie est habituellement utilisée par les banques en vue pour prévenir des attaques internes.

Dans les faits, les propriétés de plusieurs dispositifs ou mécanismes, peuvent être combinées en vue de réaliser une ou plusieurs primitives conceptuelles. Si le Zero Knowledge est parfaitement adapté pour valider l'authentification, l'intégrité peut être mise en œuvre en utilisant RSA et un certain nombre de clés symétriques (signature digitale.)

- Combinaisons et sécurités induites :

Il est inéluctable dans une analyse d'un modèle de sécurité d'évoquer certains éléments des mécanismes ou dispositifs. Lors des mises en œuvre des aspects conceptuels, l'objectif est de construire la confiance par rapport au(x) concept(s) à l'aide de ces mécanismes et dispositifs.

L'approche AXIS-CSRM et la sécurité :

- Trusted Third Party (Tierce Partie Certifiante) :

Le Trusted Third Party (tierce partie de confiance), assure un certain nombre de services entre des entités inter-communicantes. Via l'exécution correcte des protocoles, ces services offriront la propriété recherchée, à savoir soit la confiance mutuelle, soit la confiance du récepteur par rapport à l'émetteur. L'approche AXIS-CSRM est extrêmement efficace pour construire ce type de propriété car elle inclut dans sa construction les services de CONFIGURATION MANAGEMENT qui sont une généralisation du concept de Trusted Third Party.

- L'approche sémantique :

L'approche sémantique permet d'identifier avec grande précision l'objet de la confiance et le présupposé, le contexte explicite sur lequel elle repose. Le système connaît exactement les tenants et aboutissants, à savoir les profiles sous-jacents et conceptuels présents en vue d'asseoir la confiance. En d'autres termes, l'utilisateur fait confiance aux données, à la capacité d'un système à effectuer des traitements, remplir des rôles…

- Identifiants uniques :

AXIS-CSRM procure un mécanisme par lequel le CONFIGURATION MANAGEMENT et la Structure permettent de construire le modèle d'identifiant, des identifiants uniques pour les MANIFESTATIONS et les ITEMS, et des identifiants uniques pour les objets qui sont représentés par ces MANIFESTATIONS ou ces ITEMS.

- Séparation de la Déclaration d'Existence d'objets de leurs Définitions ou de leurs modèles en vue de construire la confiance.

AXIS-CSRM génère systématiquement une classe de déclaration d'existence (l'AXIS FootPrint).

De plus, AXIS-CSRM exécute une double séparation. D'une part, une Déclaration d'Existence d'Objet, et d'autre part les objets qui décrivent ou qui définissent l'objet en tant que tel ou des modèles de l'objet dont on vient de donner une définition. Ces deux éléments sont donc gérés distinctement ce qui permet de résoudre tous les types de problèmes d'identification des critères de confiance, l'objet ou les modèles de l'objet évoqués.

- Les certificats sont des documents qui donnent des informations certifiant des objets.

La plupart du temps, la certification couvre toute une série d'objets d'une manière précise. La première fonction d'un certificat est de certifier l'authenticité (Agents, Objets, Entités ou des AXES.)

Ce dernier point est peut-être le plus important de toute la section 6.6. L'approche AXIS-CSRM génère certains des documents associés à des Entités (logical entities ou physical entities) avec des nuances dans les possibilités d'expression, ce sont des certificats. Mais ces certificats peuvent également s'appliquer à toute une série d'autres éléments.

Le spatial et le temporel :

La confiance peut être bâtie sur une promesse de qualité d'une réalisation d'une intention. Certaines données à certifier sont des données ''statiques''. Ce sont des Fichiers, des Dossiers, ou des ensembles de fichiers assemblés dans des dossiers, soit le ''spatial''.

Si un utilisateur dispose d'un fichier codé en MP3, validé comme étant conforme à la norme, il peut attribuer un certificat de confiance qui offrira à un autre auditeur la qualité attendue (conforme à celle du MP3).
Cet exemple construit sur le format MP3 s'applique dans énormément de situations. A peu près toutes les primitives conceptuelles peuvent être vues tant du côté spatial que temporel. Par exemple, l'authenticité d'une personne physique pourrait être prouvée uniquement à certains moments et pas à d'autres. Certains protocoles ne permettent pas de faire la garantie ou la construction de la confiance de manière purement spatiale. Dans ce cas il faut appliquer un mécanisme temporel.

Les intentions de sécurité Security intentions

Le CD audio est un bel exemple de l'intention de la construction de mécanismes sécuritaires. En effet, la technologie embarquée vise à offrir la meilleure qualité possible même dans le cas d'une détérioration du support. Ce mécanisme ne permet nullement d'augmenter la qualité de l'audio, il dispose simplement d'une protection interne (en lecture) face aux risques de certaines dégradations de la surface optique. De même pour le MP3, mais du fait de l'intention, il n'est pas possible de modifier le codage en vue d'obtenir une qualité identique à celle d'un CD audio.

La normalisation :

Enormément d'éléments relatifs tant aux concepts qu'aux mécanismes et dispositifs de sécurité ont été normalisés par différentes institutions internationales, et en particulier au niveau européen. Il existe une norme générale, «le Green Book» qui règle les relations existantes et qui classifie les relations qui peuvent exister entre la façon de viser un certain nombre de primitives conceptuelles et leur mise en œuvre avec un certain niveau de qualité. Cela peut même concerner des exigences qui sont classiquement requises pour le militaire, ou des systèmes de sécurité de centrales nucléaires, etc.

En ce qui concerne les aspects sémantiques, les mécanismes d'accrochage des aspects purement cryptographiques et l'assurance des données elles-mêmes, sont incorporés dans les normes W3C (World Wide Web Consortium)

Sécurité intrinsèque et procédurale :

Dans certains cas, le certificat associé à un objet donne une information de qualité, de confiance de manière intrinsèque. Le certificat déclare les données fiables au niveau de l'intention.
Cependant, dans un certain nombre de cas, le résultat de la confiance est un résultat procédural. Si deux entités, Alice et Bob, sont en interaction, la confiance entre Alice et Bob résulte d'un enchaînement de messages dans le cadre d'un protocole et c'est le résultat obtenu (successful) de ce protocole qui induit la confiance.

1.1.1.1 L'usage personnel / la communication à d'autres :

Toute une série d'éléments de la sécurité peuvent être appliqués à une intention personnelle. Par un mécanisme de cryptage dont l'utilisateur détient la clé, il peut verrouiller un document à son usage exclusif.
Cependant, pour un échange entre deux personnes, il est nécessaire que l'expéditeur transmette l'information de décryptage au destinataire. Ce sont des mécanismes interpersonnels de sécurité, de confiance.

Primitives conceptuelles :

Authenticité :

L'authenticité permet de valider que des qualités attribuées à un objet ou une personne sont réelles et certifiées. Il s'agit de construire la confiance sur le fait que ce dont une personne parle est bien ce qu'elle croit être (objet ou personne, un interlocuteur au téléphone par exemple). Tout cela représente l'authenticité relative à des Agents, à des Personnes. Cela concerne également l'authenticité de centres, de domaines, d'actions, d'Autonomous Resource Entities. La question de l'authenticité est posée dès que deux entités interagissent, et ces entités peuvent être des agents (personnes physiques ou morales), mais également n'importe quel objet stocké dans des bases de données (document, fichier, etc.) ou une Autonomous eXchange Entity, un ensemble cohérent ayant les profils, les en-têtes, l'emballage, etc.

Pour ce faire, une tierce partie certifiante (Trusted Third Party) va émettre un certificat. Ce document dispose des caractéristiques cryptographiques susceptibles de certifier l'authenticité sur la base d'un certain nombre de critères. En règle générale, le certificat produit par la TTP déclare que sur la base d'un certain nombre de paramètres, l'objet ou la personne est bien ce qu'elle prétend être.
Ce document déclare par exemple que l'application Alice est bien Alice, et qu'elle est reconnaissable via la mise en œuvre d'une opération définie. Cette TTP protège contre une «impersonalisation», qui est en fait une usurpation d'identité par une autre.
Un certificat est donc lié à une identité, et il est nécessaire de procéder à une authentification de cette identité. L'objectif n'est pas de reporter tout le poids de l'authentification sur la Trusted Third Party. La plupart du temps c'est un tiers certifiant de plus haut niveau qui va délivrer un certificat authentifiant le caractère fiable de la TTP de plus bas niveau[ii].

Pour résoudre ce genre de problématique, il est possible d'établir des certificats ''croisés'' sur la base de différentes méthodes et acteurs. Dans ce cas, il est possible de déterminer un acteur de très haut niveau stable pour une longue période. Par ce mécanisme dit de ''tiroir'', il est possible de remplacer la carte à puce sans perte de fiabilité sur les actes qui ont été signés préalablement. De ce fait, le système permet la vérification de la validité des actes, et d'obtenir des modifications ou des droits d'accès dans les actes avec la nouvelle carte à puce. Tous ces mécanismes sont réglés par des protocoles éprouvés.

Ces certificats peuvent également être utilisés pour d'autres applications notamment des informations sur la qualité des données. Dans tous les cas, ces certificats doivent mentionner dans leurs paramètres le système de certification utilisé puisque l'approche conceptuelle vise à donner une confiance sur l'authenticité mise en œuvre par des mécanismes ou des dispositifs spécifiques. Et c'est cette combinaison de mécanismes, de dispositifs ou de protocoles qui va conduire à la construction de la confiance. Dans le cas d'un AXE, le système sera mentionné dans le profile dans l'en-tête.

Pour authentifier un Objet ou une Personne, il est d'usage d'utiliser des caractéristiques humaines suivantes :

- Ce qu'un individu est : un certain nombre de caractéristiques de l'humain (personne physique avec un corps, des bras, des mains avec une empreinte digitale, …) C'est également le cas pour la vue, avec une caractéristique commune qui est l'iris même s'il constitue un identifiant unique. Il faut également tenir compte de la composante ''temps'' qui fait varier par exemple la couleur des cheveux.
- Ce qu'un individu connaît : par exemple le code secret de sa carte bancaire, le nom d'un animal, … (mécanismes utilisés pour sécuriser et authentifier des accès à des applications.)
- Ce qu'un individu sait faire : jouer du piano, taper à la machine (identification d'une personne grâce au rythme de frappe sur le clavier.)
- Ce qu'un individu possède : une carte à puce dont la possession est réputée honnête, un permis de conduire, un abonnement.
- Ce qu'un individu occupe (spatio-temporel) : une maison, un emplacement de parking…

Les certificats peuvent donc valider l'authenticité en se servant de toute une série de caractéristiques mais la clé de voûte du certificat c'est l'identité authentifiée par ce même certificat. Il faut mettre en œuvre des moyens de réaliser l'association de tous ces paramètres. Dans certains cas, le certificat peut être ultra simple s'il s'agit d'une carte à puce avec interaction entre un objet et des calculs effectués au niveau de la carte. Il n'y a pas d'intervention humaine explicite mais bien des agents informatiques.

Dans le cas où la procédure veille à valider que l'Agent est bien une personne physique, c'est une autre procédure d'authentification qui est mise en œuvre, à savoir la reconnaissance par l'humain de caractères dessinés dans une image. Des mécanismes similaires existent à partir d'un nombre émis au hasard par une boîte vocale.

Tous ces mécanismes sont comme toujours contournables mais néanmoins cela devient de plus en plus difficile.

Unicité :

Il s'agit bien sûr du caractère de ce qui est unique, qui est seul dans une Classe donnée. L'unicité est extrêmement importante pour toute une série de domaines dont celle de la gestion des droits. Il s'agit de déterminer avec un haut degré de fiabilité qu'un ITEM (Objet, Personne physique, Fichier, …) défini dans le cadre d'AXIS-CSRM est effectivement unique. Dans le cas d'une personne physique la preuve d'authenticité découle du fait que les humains ne peuvent pas être clonés.

Le problème de l'authenticité est plus difficile à résoudre pour des Objets (des statues, des bijoux, des dvd, des cd, des livres ou des fichiers comme objets informatiques), mais des solutions sont disponibles à la fois pour des Objets statiques ou dynamiques.

Ce qui est vrai pour les objets est aussi vrai pour les modèles d'objets, le problème d'unicité n'est pas uniquement lié à l'unicité de l'objet mais aussi à ses modèles.

La manière de garantir l'unicité grâce à une technique est fort proche de celle utilisée pour garantir l'authenticité. Le droit d'assister à un concert ou à une pièce de théâtre, sur le siège n°26 de la troisième rangée garantit au titulaire du billet le fait de pouvoir disposer de ce siège durant toute la durée du spectacle, personne d'autre n'a le droit d'utiliser cette place. L'unicité du siège garantit l'unicité de l'événement spatio-temporel qui est le droit d'assister à un spectacle à tel endroit, dans telle salle, un tel jour …

Vie privée (Privacy) :

La vie privée concerne tout ce qui est d'ordre strictement personnel. C'est la façon de construire le fait que les données publiées sont protégées par rapport à la vie privée d'un individu. Le système garantit l'accès unique via des techniques de cryptographie ou autres. De même pour une communauté d'utilisateurs qui aura accès à des informations partagées (rédaction, groupement, association, ..)

Qualités :

- Intégrité :

Si l'information a été représentée par des données, comment déterminer si elles sont restées intègres ? L'encapsulation des données par un système de protection destiné à garantir leur intégrité, procure une mécanique de qualité. Ce mécanisme de qualité (comme le reste de la division par 97 d'un numéro de compte bancaire) donne une information certaine d'intégrité des bits. Dans certains cas il est nécessaire de garantir une intégrité de plus haut niveau à l'aide de codes correcteurs d'erreurs.

De nouveau il existe des technologies et des normes sur la façon d'assurer l'intégrité. Par exemple, un AXE peut être garanti intègre dans sa globalité mais des mécanismes d'intégrité peuvent permettre de descendre à des niveaux plus bas comme celui de la taille d'un fichier ou les caractéristiques d'un enregistrement programmé.

- Conformité (Compliance)

La conformité est une caractéristique en rapport avec un modèle. Par exemple, un fichier produit dans le format MP3 est-il bien conforme à la norme MPEG-1/2 Audio Layer 3 de l'ISO ? Dans ce cas, tout lecteur de fichier MP3 conforme à la norme sera capable de le présenter.

- Adéquation :

L'adéquation est une conformité au contexte. La qualité proposée par un fichier MP3 suffit largement pour une écoute dans un environnement personnalisé et relativement bruyant. Il va de soi que ce même MP3 sera tout à fait insuffisant pour satisfaire l'adéquation d'une diffusion dans votre living-room ou dans une salle de concert.

- Représentativité :

La représentativité concerne la conformité des données en question par rapport à l'attente d'un utilisateur.

- Disponibilité :

Un SLA (Service Level of Agreement) définit les modes d'accès à de l'information dans des délais déterminés. C'est une autre assurance de qualité pour laquelle des certificats peuvent être émis. Et en cas de disfonctionnement constaté, des pénalités ou des dédommagements peuvent être envisagés (conventions liées aux certificats.)

- Persistance :

La gestion de la persistance des données réfère au mécanisme responsable de la sauvegarde et de la restauration de données. Ces mécanismes font en sorte qu'un programme puisse se terminer sans que ses données et son état d'exécution ne soient perdus. Cela concerne également les tiers fiables et les identifiants. La persistance des données en archivage est une des caractéristiques essentielles et les certificats peuvent couvrir ce genre de risques en cas de défaillance du prestataire de service.

- Traitement (Processability)

La ''processability'' est plus complexe car elle garantit non seulement la disponibilité de l'information en fin de processus mais de plus, l'accès aux processus et aux protocoles associés.
Cela signifie entre autres que les choix technologiques sont tels que les calculs nécessaires prévus par les protocoles peuvent être effectués et que le traitement assure l'aboutissement de ces opérations. Le non-aboutissement équivaut à une rupture de confiance dans le mécanisme.

- Normalisation

Les certificats peuvent fort bien déclarer, comme on l'a vu dans l'exemple de conformité, que les données en question ont été effectuées conformément à une norme (par exemple les adresses sont exprimées suivant un mécanisme normé).

- Automation / Autonomie – Automation / Autonomy

Toute l'information requise est disponible et groupée par un mécanisme d'emballage (un wrapper) qui peut être automatisé. Idéalement, toutes les fonctions de CONFIGURATION MANAGEMENT doivent être telles qu'elles puissent s'exécuter de manière autonome et être exécutées dans des Tamper-Resistant Devices.

Communication & Combinaisons (AXE) :

- Signature

La plupart du temps, le travail de construction de la confiance concerne d'abord la personne qui construit, qui crée l'information. L'interaction avec des tiers certifiants va progressivement donner de la confiance aux utilisateurs.

Pour ce faire, toute une série de systèmes ont été conçus en vue de construire la confiance entre des Agents communicants. Le plus connu de ceux-là est la combinaison entre un protocole RSA et l'incorporation d'une clé secrète symétrique dans ce protocole, ce qui donne toute une série de caractéristiques dont la plus connue de toutes est la ''signature''. Un document signé par un agent ou une personne physique et validé par une tierce personne, sera doté d'une double confiance. La première concerne l'authenticité du signataire et la seconde l'intégrité du document signé par l'agent. C'est un mécanisme intitulé la signature digitale.

La signature peut également faire l'objet d'une délégation de pouvoir, un certificat qui donne mandat à une autre personne (le proxy) pour remplir certaines missions. Il existe des protocoles qui permettent de donner les validités de signature pendant une certaine période à un proxy. L'exemple typique est l'administrateur d'une personne morale, durant la période où il dispose des droits d'administrateur (signer pour représenter seul ou en combinaison avec d'autres administrateurs pour des tâches définies dans le statut.)

Tout cela est représentable comme des documents qui peuvent être incorporés et attachés à des Logical Entities ou des Physical Entities, ou incorporés dans des AXES, et en particulier des contrats, des conventions etc.

- Non répudiation :

Documents (Méta-Documents – Certificats – Documents signés – Conventions)

Méta-documents

Il existe des certificats, qui sont en quelque sorte des formulaires. Typiquement un contrat vierge où l'acheteur signe et s'acquitte du payement d'un bien. Les méta-documents sont donc incorporés dans les Profiles et seules des instances de ces méta-documents donnent la certification sur la garantie ou la confiance.

Certificats :

Les certificats les plus importants sont ceux qui concernent l'authenticité. Ces certificats sont des documents attachés à des Entités (Logical ou Physical Entities.)

Documents signés :

Le document existe en soi mais il existe des protocoles par lesquels la signature est incorporée dans le document. Il existe d'autres types de protocoles pour lesquels c'est la combinaison du document avec le certificat signé qui conduit à la signature de ce document. C'est souvent le cas pour d'autres types de protocoles comme ceux qui nécessitent plusieurs signatures par rapport à un même document. Il y a alors un lien non ambigu entre le document signé et le second qui comprend l'ensemble des signatures des personnes physiques.

Conventions :

Tous les cas de gestion des droits sont couverts par des conventions (en fait un méta-document complété.) Le plus connu de tous est le « **contrat d'exploitation directe »** (une personne détentrice des droits sur une œuvre, cède certains droits à un tiers en vue de son exploitation.

Le **contrat de brokerage** est une autre forme de convention dans laquelle un titulaire de droits confie à un tiers la commercialisation des ITEMS. Toutes les plates-formes connues telles que I-Tunes par exemple ont des contrats avec les détenteurs de droits des œuvres qui sont diffusées via cette plate-forme. Un contrat de brokerage unit donc les détenteurs de droits et la plate-forme I-Tunes en vue de permettre à cette dernière d'exploiter les contenus mis à disposition.

Les **certificats de contribution à une œuvre** ont comme objet le fait de qualifier une personne en termes de détenteur de droits (producteur, auteur ou acheteur des droits liés à la commercialisation de l'œuvre, etc.) C'est à ce niveau que se situe une différence majeure d'interprétation des droits entre l'auteur reconnu d'une œuvre (Citizen Kane, réalisé par Orson Welles) et le copyright qui reconnaît la personne physique ou morale qui détient les droits d'exploitation (Sony Music.)
Les certificats de contribution ou certificats d'acquisition de droits peuvent nuancer ce propos en déclarant qu'Orson Welles reste l'auteur de Citizen Kane, mais que grâce au contrat passé entre Sony et Orson Welles, Sony a acquis tous les droits de commercialisation et d'exploitation.

En amont d'une production, le fait d'engager un acteur lors d'un casting pour un film génère contrat fixe les règles du jeu et les rétributions liées à l'exploitation. La prestation d'un musicien, un violoncelliste dans un orchestre, génère des droits dérivés dans le cadre de la loi française.

Grâce aux mécanismes de l'approche AXIS-CSRM liés au CONFIGURATION MANAGEMENT, aux mécanismes d'identification unique et des techniques mises en place, il est possible de bâtir un modèle de sécurité relativement complet qui génère des méta-documents et des instances de documents (certificats, conventions, documents signés etc) qui sont attachés aux entités (documents attachés ou méta-documents incorporés dans des Profiles.) Tous ces mécanismes peuvent donc construire la confiance, il suffit pour cela de créer des méta-documents qui sont liés à un objectif précis et d'en faire les instances associées à des entités ou des objets informatiques.

---

[i] La représentation du son sur un CD audio constitue un autre exemple de correction sophistiquée des erreurs malgré des détériorations du support ou des erreurs de lecture car les données sont représentées de manière optique, ce qui fragilise le système. Lors du développement du CD audio, la société Phillips a mis en place un système extrêmement sophistiqué pour détecter des erreurs prédictibles et les corriger.

Pour le développement du format WAVE qui est équivalent en qualité au CD audio, la société IBM n'a pas intégré de système de correction d'erreurs. On peut cependant adjoindre un fichier WAVE avec des informations annexes en vue d'effectuer des corrections d'erreurs mais cette modalité ne figure pas dans la norme.

[ii] Exemple : dans la carte à puce d'identité belge, il y a un certificat à l'intérieur de la carte qui est émis par le Ministre de l'Intérieur qui déclare que le certificat émis par la commune qui délivre la carte d'identité est bien correct. Lors de l'utilisation de cette carte d'identité pour signer un document, le lecteur du document signé informatiquement, c'est en fait le Ministre de l'Intérieur ou son délégué qui valide l'acte. Ces certificats sont établis pour des durées déterminées (la carte à puce émise par une banque ou une administration comporte également une date d'expiration.)