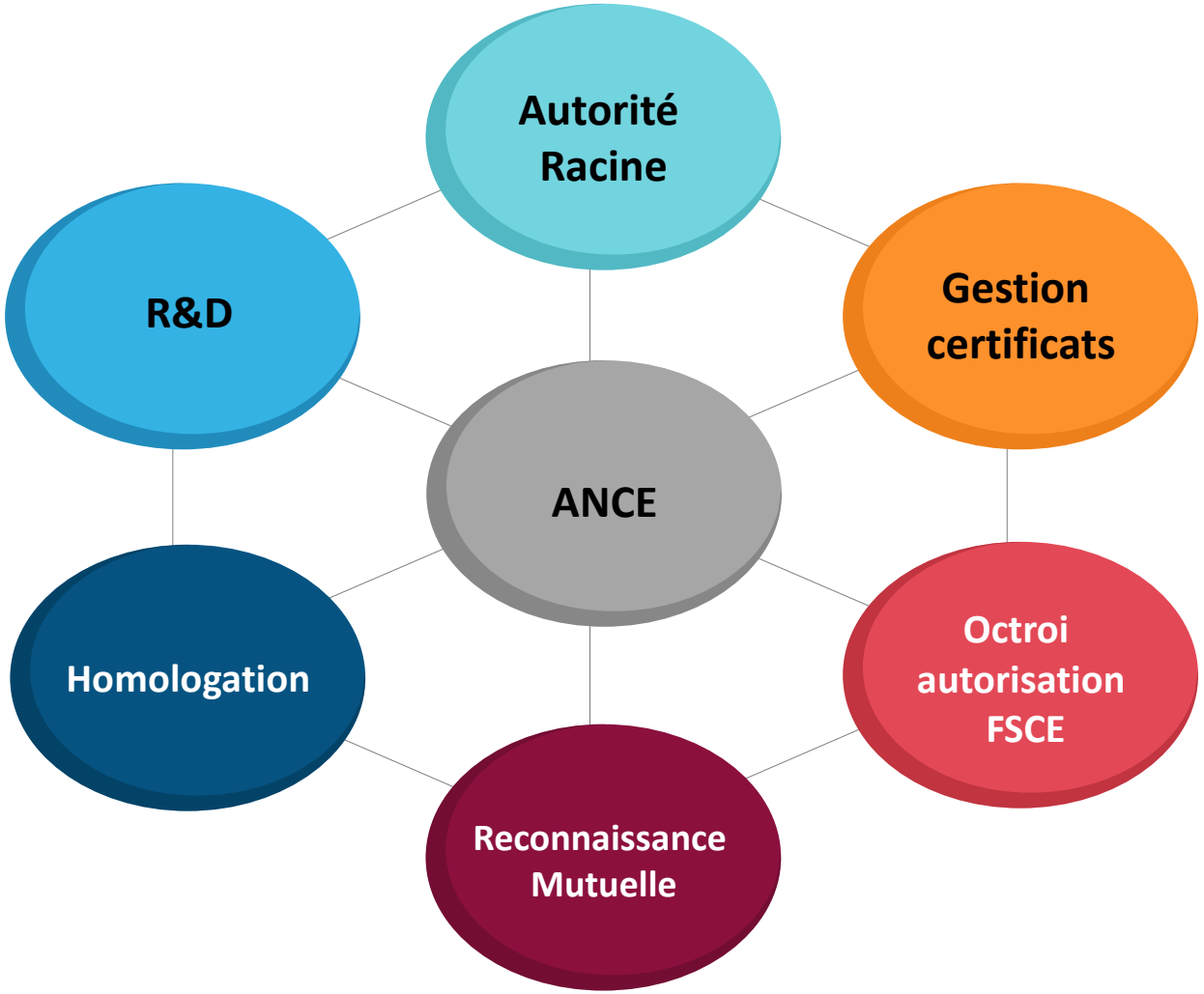
Conformité des Autorités de Confiance aux Standards Internationaux (Webtrust, ETSI, ISO, …)

Agence Nationale de Certification Electronique

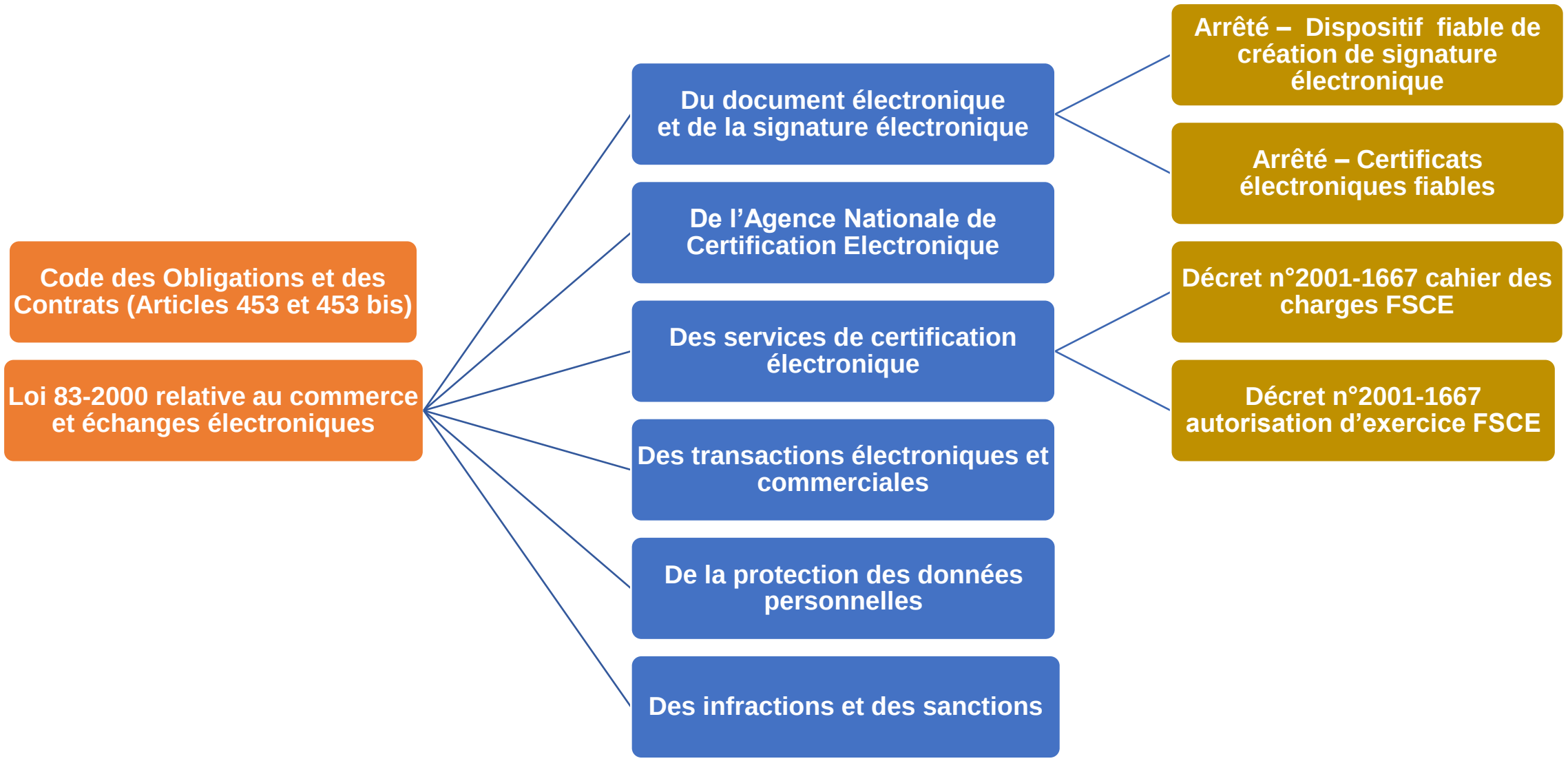
Séminaire TAIEX sur la protection
des systèmes d'information
d'importance vitale

25-26 Septembre 2019
Golden Tulip El Mechtel, Tunis, Tunisie

Agence Nationale de Certification Electronique



Cadre Réglementaire



Services de Confiance

2016 — Mise à Niveau PKI Nationale

ID-Trust · Code · SSL · VPN · Horodatage

2017 — Cachet Electronique Visible

Enterprise-ID · TN CEV · QR-Sign · TunSign

2018 — Signature Mobile

QR-Check · Mobisign

2019 — Lancement officiel DigiGO

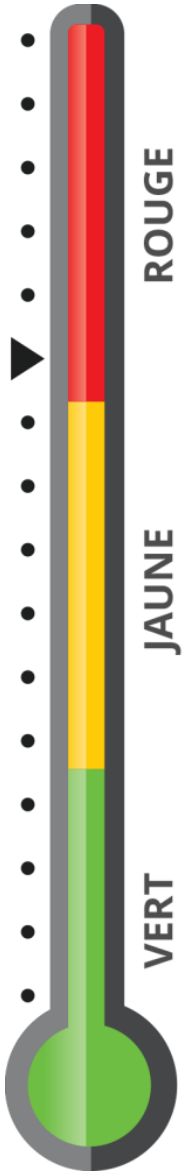
DIGIGO

2020 — Archivage Electronique Authentification Biométrique

4 Produits
1 service

6 Produits
9 services

Signatures Electroniques



Signature électronique

«signature électronique», des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer;

Signature Avancée

« signature électronique avancée » :
a)être **liée au signataire de manière univoque**;
b)permettre **d'identifier le signataire**;
c)avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous **son contrôle exclusif**; et
d)être liée aux données associées à cette signature de telle sorte que **toute modification** ultérieure des données **soit détectable**.

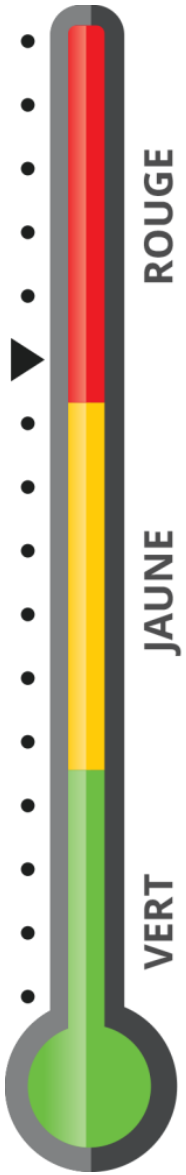
Signature Qualifiée

«signature électronique qualifiée», une signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié, et qui repose sur un certificat qualifié de signature électronique.

Certificat Qualifié

QSCD

Certificat SSL



DV SSL

Domain Validation : L'autorité de certification (AC) s'assure uniquement que vous êtes le propriétaire d'un domaine spécifique en utilisant les informations contenues dans le WHOIS

OV SSL

Organisation Validation : Les certificats OV sont requis pour les sites de vente en ligne. Un certificat OV authentifie le propriétaire du site et requiert des informations commerciales légitimes pour cette société. L'autorité de certification vérifie que vous êtes propriétaire du domaine, mais également que que votre entreprise figure dans une base de données du registre des entreprises.

EV SSL

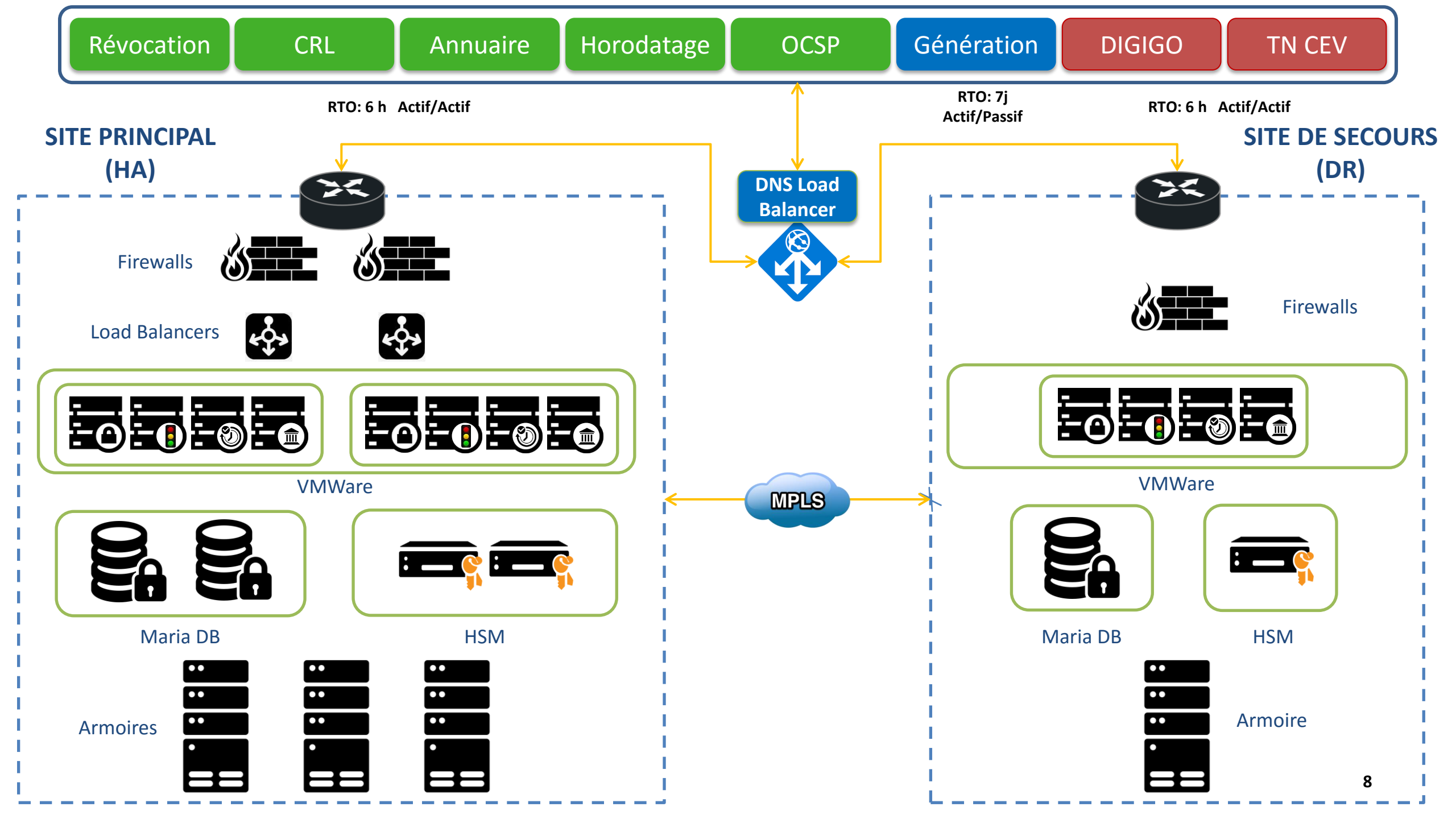
Extended Validation : Vérifications du contrôle de nom de domaine et de l'existence physique, légale et opérationnelle de l'entreprise encore plus avancée

Certificat SSL

Domain Validation : L'autorité de certification (AC) s'assure uniquement que vous êtes le propriétaire d'un domaine spécifique en utilisant les informations contenues dans le WHOIS

Organisation Validation : Les certificats OV sont requis pour les sites de vente en ligne. Un certificat OV authentifie le propriétaire du site et requiert des informations commerciales légitimes pour cette société. L'autorité de certification vérifie que vous êtes propriétaire du domaine, mais également que que votre entreprise figure dans une base de données du registre des entreprises.

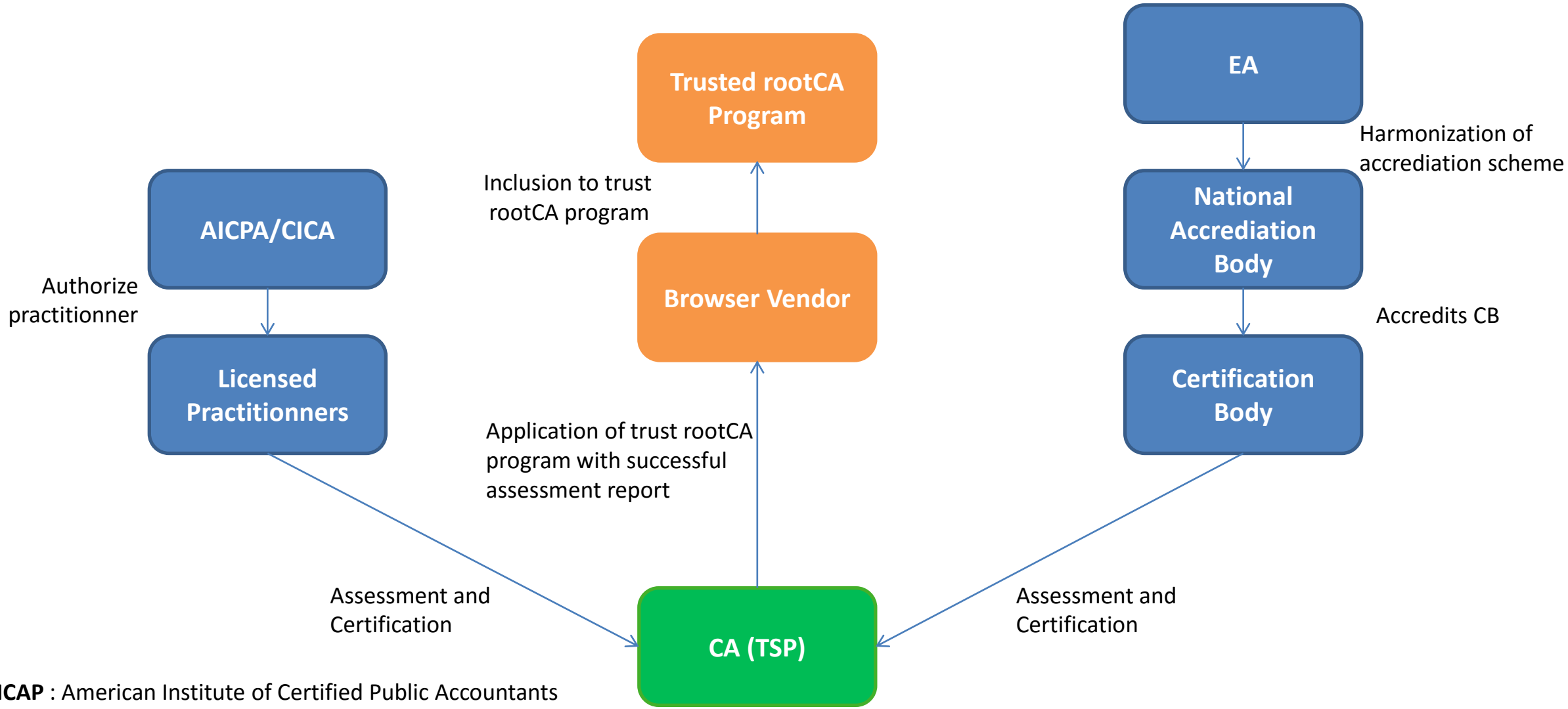
Extended Validation : Vérifications du contrôle de nom de domaine et de l'existence physique, légale et opérationnelle de l'entreprise encore plus avancée


Révocation
CRL
Annuaire
Horodatage
OCSP
Génération
DIGIGO
TN CEV
RTO: 6 h Actif/Actif
RTO: 7j
Actif/Passif
RTO: 6 h Actif/Actif
SITE PRINCIPAL
(HA)
SITE DE SECOURS
(DR)
DNS Load
Balancer
Firewalls
Load Balancers
VMWare
MPLS
Maria DB
HSM
Armoires
Firewalls
VMWare
Maria DB
HSM
Armoire

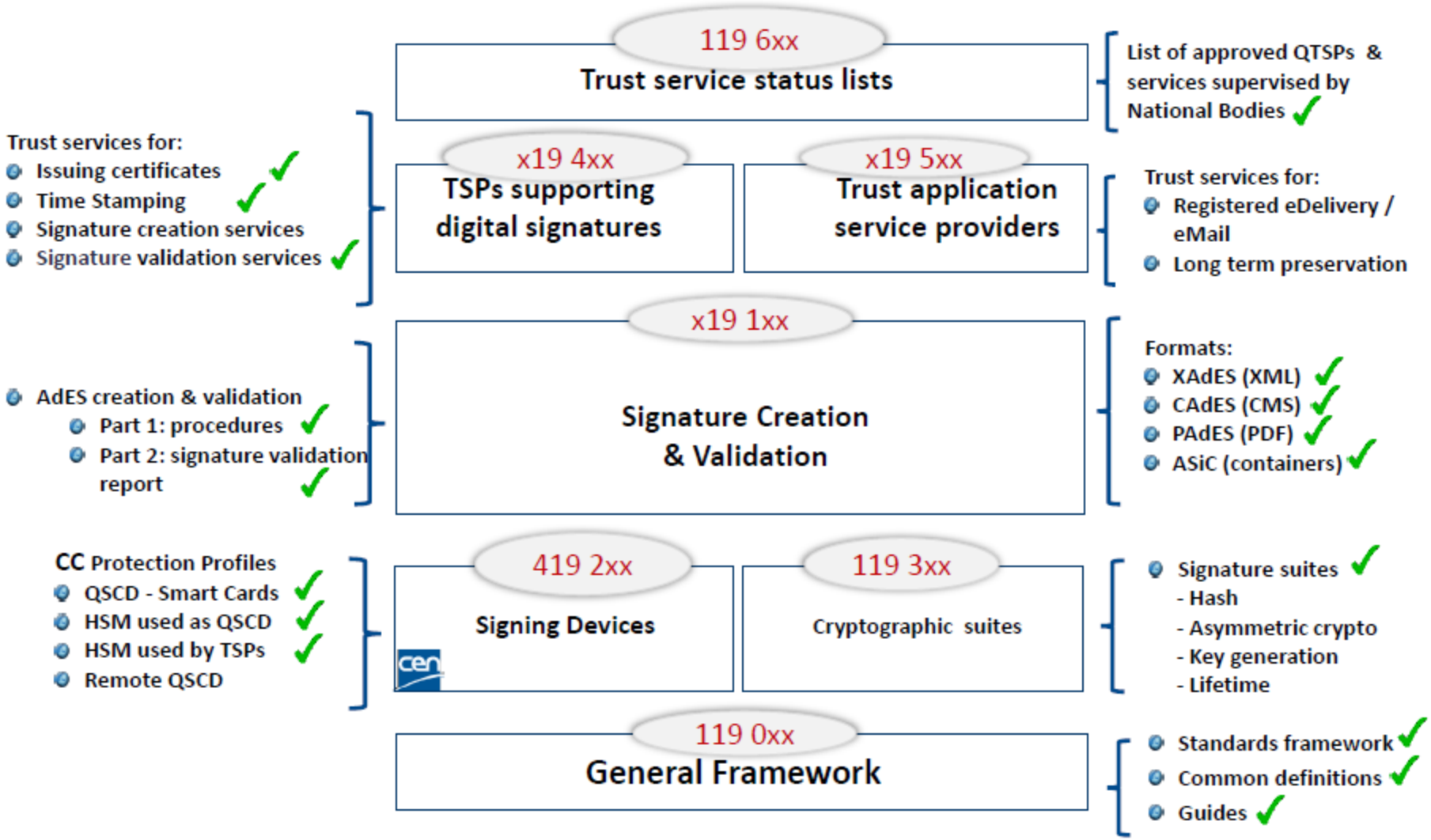
Nos Qualifications

- **Depuis 2015 :**
  - **ETSI EN 102 042** Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates
- **Depuis 2016 :**
  - **ETSI EN 319 411-1** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
  - **ETSI EN 319 411-2** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
  - **ETSI EN 319 421 V1.1.1**: Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for trust service providers issuing time-stamps
- **De 2015 à 2018**
  - **ISO 9001:2008 Quality Management System - Requirements**
- **Depuis 2018**
  - **ISO 9001:2015 Quality Management System - Requirements**
  - **ISO/IEC 27001:2013 Information Security Management**
- **En cours :**
  - **Webtrust Principles And Criteria For Certification Authorities 2.2**
  - **WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.4.1**

Inclusion to trust rootCA programs



AICAP : American Institute of Certified Public Accountants
CICA : Canadian Institute of Chartered Accountant
ETSI: European Telecommunications Standards Institute


119 6xx
Trust service status lists
List of approved QTSPs & services supervised by National Bodies
Trust services for:
Issuing certificates
Time Stamping
Signature creation services
Signature validation services
x19 4xx
TSPs supporting digital signatures
x19 5xx
Trust application service providers
Trust services for:
Registered eDelivery / eMail
Long term preservation
x19 1xx
AdES creation & validation
Part 1: procedures
Part 2: signature validation report
Signature Creation & Validation
Formats:
XAdES (XML)
CAdES (CMS)
PAdES (PDF)
ASiC (containers)
CC Protection Profiles
QSCD - Smart Cards
HSM used as QSCD
HSM used by TSPs
Remote QSCD
419 2xx
Signing Devices
119 3xx
Cryptographic suites
Signature suites
- Hash
- Asymmetric crypto
- Key generation
- Lifetime
119 0xx
General Framework
Standards framework
Common definitions
Guides

Programme Webtrust

Le programme **WebTrust** à l'intention des AC vise à accroître la confiance des consommateurs concernant le commerce électronique et la technologie ICP . Ce programme inclut les principes énumérés ci-dessous auxquels l'AC doit se conformer:

- ***Politique de Certification et Déclaration des Pratiques de Certification (PC/DPC)***
  - L'AC divulgue ses pratiques de confidentialité des informations et des activités de gestion du cycle de vie des clés et des certificats et fournit ses services conformément à ses pratiques divulguées.
- ***Intégrité du service***
  - Les informations du porteur de certificat sont correctement authentifiées (activités d'enregistrement) et
  - L'intégrité des clés et des certificats qu'elle gère est établie et protégée tout au long de leur cycle de vie.
- ***Contrôles opérationnels de l'AC***
  - Les informations sur l'abonné et la partie de confiance sont restreintes et protégées
  - La continuité des opérations de gestion des clés et des certificats est maintenue
  - Le développement, la maintenance et l'exploitation des systèmes CA sont dûment autorisés et effectués de manière à préserver leur intégrité.

Processus d’Audit Webtrust

Le processus d'audit comprend généralement les phases suivantes:

- **Planification** – Définir le calendrier général de l'audit, fournir la liste des documents, examiner la PC / DPC et les autres politiques / procédures avant le travail sur le terrain.
- **Travail sur le terrain** - Organiser des réunions avec des personnes clés, observer les processus, inspecter les configurations, rassembler des preuves d'audit
- **Analyse hors site** - Analyse des informations recueillies pendant et après le travail sur le terrain
- **Reporting** - Préparation du rapport d'audit

Summary of WebTrust for CAs Criteria Topics

CA BUSINESS PRACTICES DISCLOSURE (CP/CPS)		
CA ENVIRONMENTAL CONTROLS	**CA KEY MANAGEMENT**	**CERTIFICATE LIFE CYCLE MANAGEMENT**
• CP/CPS Management • Security Management • Asset Classification and Management • Personnel Security • Physical and Environmental Security • Operations Management • System Access Management • Systems Development and Maintenance • Business Continuity Management • Monitoring and Compliance • Event Journaling	• CA Key Generation • CA Key Storage Backup and Recovery • CA Key Escrow (optional) • CA Key Usage • CA Key Archival • CA Key Destruction • CA Cryptographic Device Life Cycle Management • CA-Provided Subscriber Key Management Services (optional)	• Subscriber Registration • Certificate Rekey/ Renewal Certificate Issuance • Certificate Distribution • Certificate Revocation • Certificate Suspension (optional) • Certificate Status Information Processing • Integrated Circuit Card Life Cycle Management (optional)

Autorité Enregistrement Délégué

Autorité Enregistrement Central

Autorité Certification

1. Demande de certificat (Dossier Papier)

2. Envoi de requête

4. Remise du certificat

3. Génération sur QSCD

5. Publication de l'état des certificats

6.Authentification et Signature par Certificat

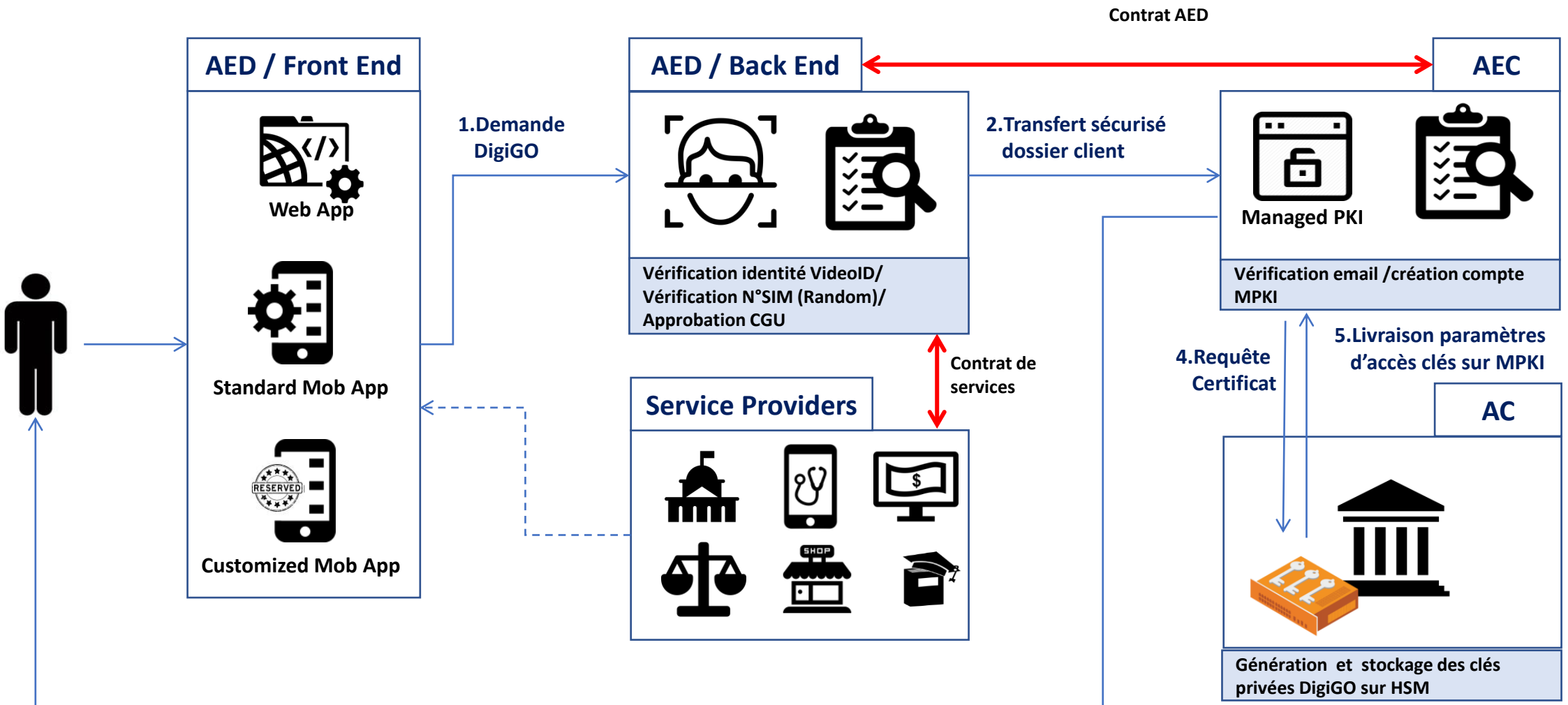
Fournisseur de services

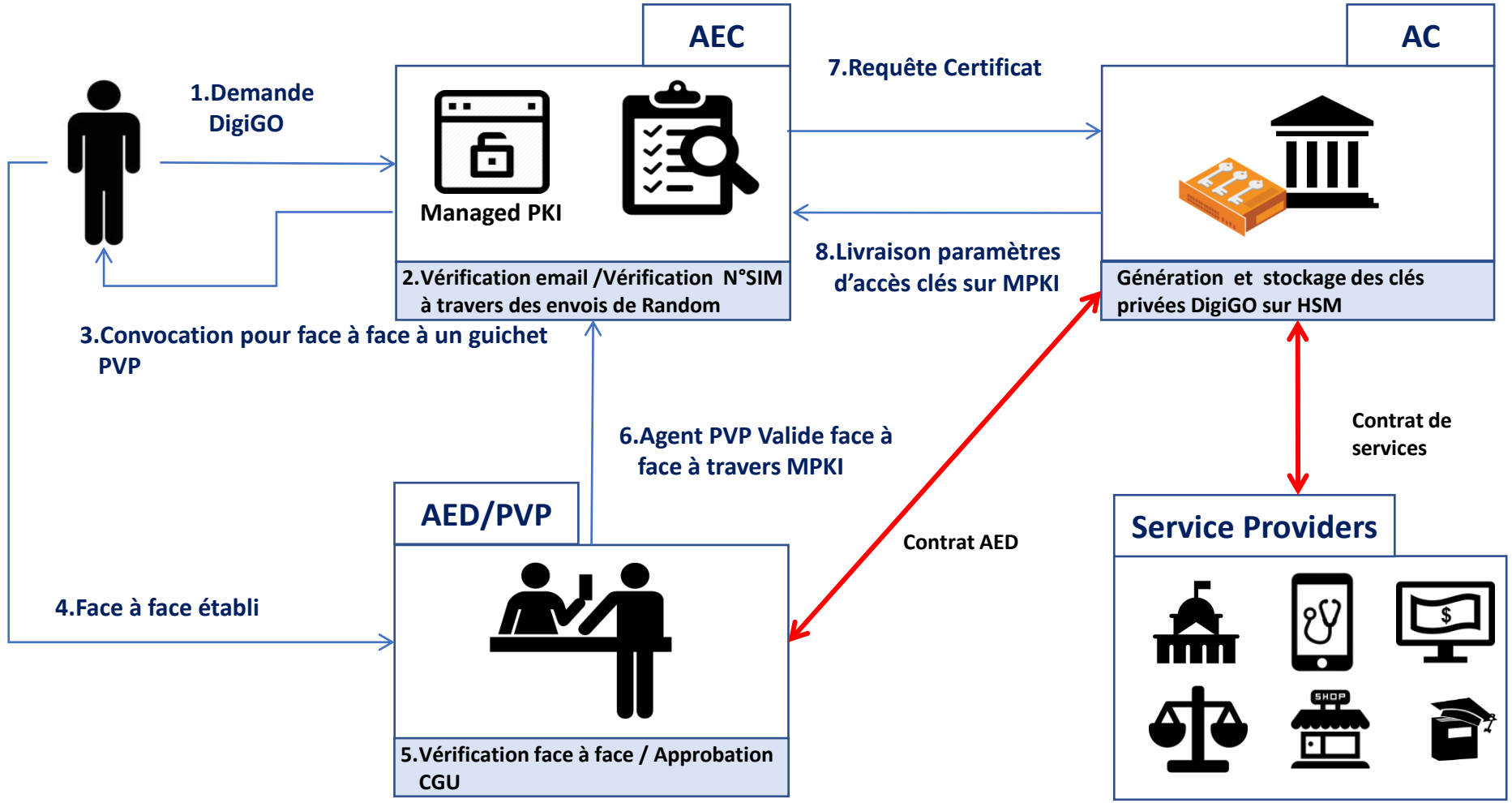
7. Vérification de la validité du certificat

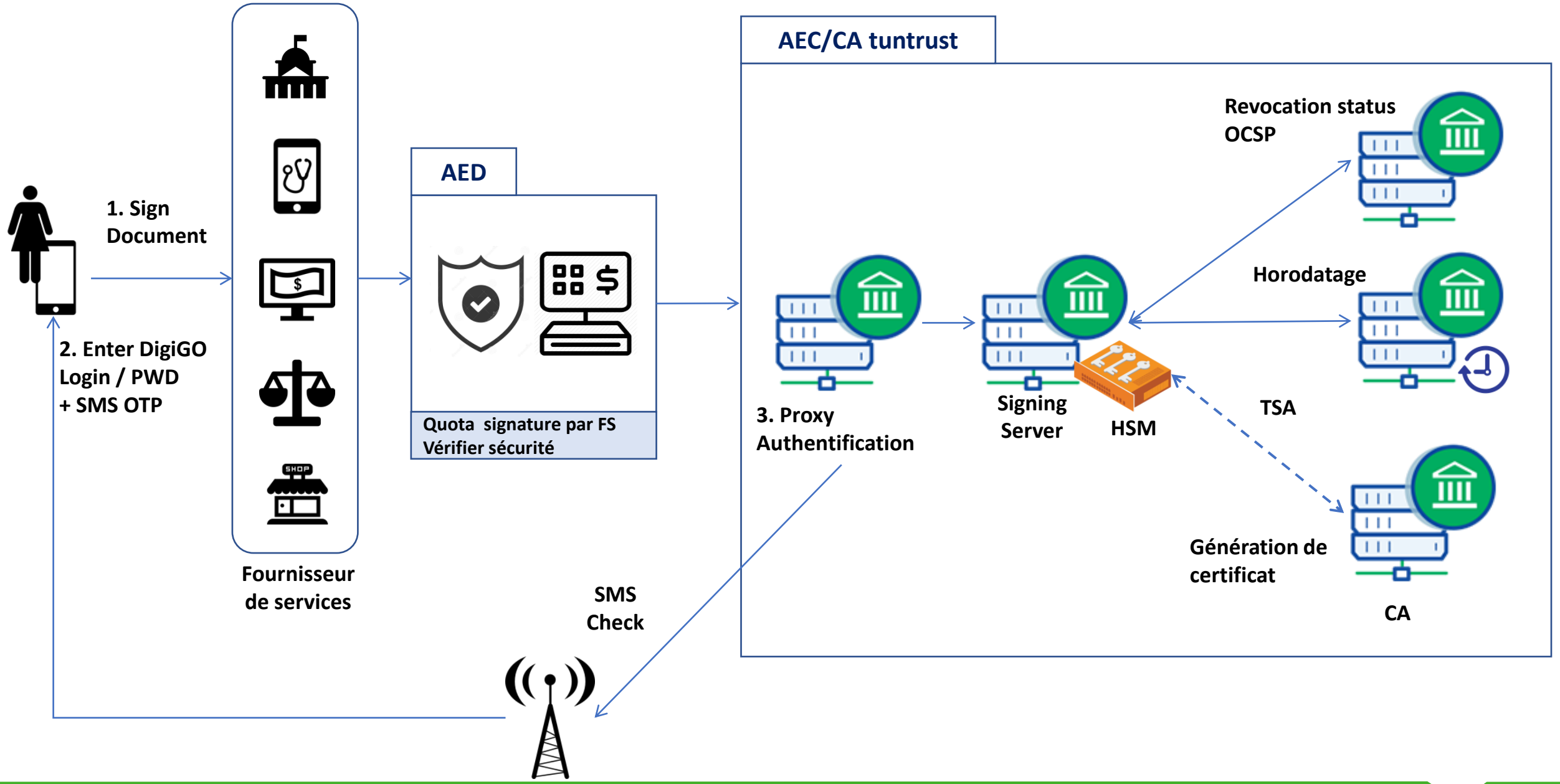
Publication

Liste des certificats révoqués

Liste des certificats valides


Contrat AED
AED / Front End
Web App
Standard Mob App
Customized Mob App
1.Demande DigiGO
AED / Back End
Vérification identité VideoID/
Vérification N°SIM (Random)/
Approbation CGU
2.Transfert sécurisé dossier client
AEC
Managed PKI
Vérification email /création compte MPKI
Contrat de services
Service Providers
4.Requête Certificat
5.Livraison paramètres d'accès clés sur MPKI
AC
Génération et stockage des clés privées DigiGO sur HSM
3. Vérification email et activation compte MPKI sur canal différent


AEC
AC
1.Demande DigiGO
Managed PKI
7.Requête Certificat
8.Livraison paramètres d'accès clés sur MPKI
2.Vérification email /Vérification N°SIM à travers des envois de Random
Génération et stockage des clés privées DigiGO sur HSM
3.Convocation pour face à face à un guichet PVP
6.Agent PVP Valide face à face à travers MPKI
Contrat de services
AED/PVP
Contrat AED
Service Providers
4.Face à face établi
5.Vérification face à face / Approbation CGU


1. Sign Document
2. Enter DigiGO Login / PWD + SMS OTP
Fournisseur de services
AED
Quota signature par FS
Vérifier sécurité
AEC/CA tuntrust
Revocation status OCSP
Horodatage
3. Proxy Authentification
Signing Server
HSM
TSA
Génération de certificat
CA
SMS Check