WAVESTONE

Les PKI et la signature électronique

Vers la dématérialisation des échanges

Octobre 2018 | Kévin GUÉRIN & Nacim BEZ | Telecom Sud Paris

TELECOM SudParis

Dans un monde où la capacité à se transformer est la clé du succès, nous éclairons et guidons nos clients dans leurs décisions les plus stratégiques

Des clients leaders dans leur secteur

2 800 collaborateurs dans 8 pays

Parmi les leaders du conseil indépendant en Europe, n°1 en France

Paris | Londres | New York | Hong Kong | Singapour* | Dubaï* | São Paulo*
Luxembourg | Madrid* | Milan* | Bruxelles | Genève | Casablanca | Istanbul* | Edimbourg
Lyon | Marseille | Nantes

* Partenariats

Une capacité unique à combiner expertise sectorielle, connaissance des fonctions de l'entreprise et maîtrise des technologies

FONCTIONS

Stratégie

Management & financement de l'innovation

Marketing, ventes & expérience client

People & change

Finance, risques & achats

Operations & logistique

SECTEURS

Banque & assurance

Télécoms & média

Biens de consommation & distribution

Industrie

Énergie & utilities

Transport & voyages

Immobilier

Secteur public & institutions internationales

TECHNOLOGIES

Stratégie digitale & SI

Technologies digitales & émergentes

Architecture SI & data

Cybersécurité & confiance numérique

Réussir sa **transformation numérique** grâce à la **confiance numérique**

500+
Consultants & Experts

1,000+
Missions par an dans plus de **20** pays

Nos clients
COMEX, Métier, CDO, CIO, CISO, BCM

UNE EXPERTISE EPROUVEE

- Stratégie et Conformité
- Transformation métier sécurisée
- Architecture et programme sécurité
- Identité, Fraude et Services de Confiance
- Tests d'intrusion & Réponse à incident
- Continuité d'Activité & Résilience
- SI Industriel

NOS DIFFERENCIATEURS

- Connaissance des risques métier
- Méthodologie AMT pour les schémas directeurs
- Radars Innovation et Start-ups
- CERT-W
- Bug Bounty by Wavestone

Des références de tout premier plan, et un retour d'expérience unique

SOCIETE GENERALE
Stratégie cybersécurité du groupe

BARCLAYS
Programme de remédiation cybersécurité

ALLIANZ - WORLDWIDE PARTNERS
Mise en conformité RGPD à l'échelle international

SANOFI
Programme de sécurisation des SI industriels

SAINT-GOBAIN
Réponse à incident sur crise cyber

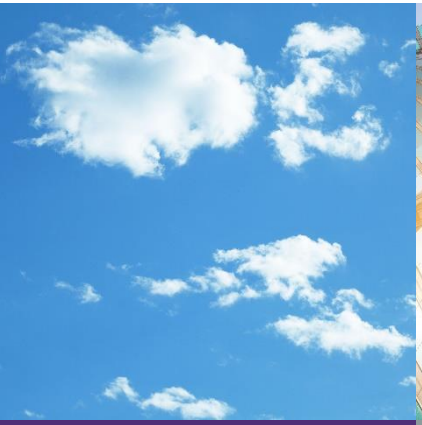
SOWEE - EDF GROUP
Audit et architecture sécurisée cloud & IoT

EDF
Stratégie Customer IAM et déploiement

SOCIETE GENERALE
Lutte contre la fraude grâce au Machine Learning

ENISA - EUROPEAN SECURITY AGENCY
Promotion des start-ups sécurité en Europe

Nous anticipons les tendances pour guider vos réflexions



CLOUD

Adopter un nouveau modèle de sécurité pour prendre en compte la réalité des déploiements

INFRASTRUCTURES CRITIQUES
(LPM/NIS, NYDFS…)

Identifier le périmètre adéquat pour limiter les impacts tout en garantissant la sécurité nationale

PROGRAMMES CYBERSECURITE

Définir son propre Framework inspiré des standards internationaux (NIST, ISO…) pour reporter de manière homogène au Board et régulateurs

SURVEILLANCE & ANTI-FRAUDE

Rendre disponible le socle technique du SOC aux métiers pour compléter leur anti-fraude sur les chaines transactionnelles critiques

CYBER RESILIENCE

Inclure un scenario d'attaque du SI à grande échelle dans le PCA, et se tester régulièrement

Nous accélérons les start-ups cybersécurité pour construire et animer un écosystème d'open-innovation

ALSID

Une solution de cyberdéfense conçue pour les décideurs afin de détecter les failles des entreprises avant les hackers

Citalid CYBERSÉCURITÉ

Une solution de cyber threat intelligence tirant parti de marqueurs techniques, géopolitiques, économiques et sociaux pour anticiper les cyber menaces et quantifier les risques

SKEY3CODE

Proposition d'une solution d'authentification forte pour les transactions et de sécurisation des applications.

sqreen

Sqreen renforce la sécurité des applications web de façon robuste, continue et transparente.

Au sein de la **communauté sécurité** tout au long de l'année

@risk_insight
#Risque #Cyber #PCA
#ID #Numérique #Conformité

@secuinsider
#Menace #PenTest
#DFIR #Malware #Conf

Venez nous rencontrez !

Octobre	Les Assises de la sécurité (Monaco) *Cybersécurité et COMEX : convaincre et démontrer l'efficacité*
Novembre	Cyber Security Connect UK (Monaco) *Security in 2025: how to adapt your approach to cope with full cloud and agile-at-scale?*
	Bsides Lisbon (Lisbonne, Portugal) *Active Directory Security: 8 (very) low hanging fruits and how to smash those attack paths*

Nos derniers ateliers

COMEX	Comment démontrer l'efficacité et la confiance ?
Intelligence artificielle	Menace ou opportunité ?
SOC/CERT	Quel modèle organisationnel ?
SI Industriel	Priorité à la gouvernance
Cyber-résilience	Quelle stratégie adopter ?
CIAM	Vers de nouvelles opportunités dans l'IAM
Cloud	Les facteurs clés de succès pour un déploiement industriel

Nos dernières publications

GDPR/Vié privée	1 an de travaux, quel bilan en tirer ?
Radar du RSSI	Anticiper pour mieux prioriser
Fraude en ligne	Nouvelles méthodes de lutte contre la fraude bancaire en ligne
Internet des Objets	Les 4 dimensions de la sécurité des objets connectés
Benchmark Audit	Bilan de la sécurité des sites web en France
API	Quelle recette pour sécuriser ses API ?
Cyber-résilience	Plier pour ne pas rompre
Start-ups cybersécurité	Un écosystème en pleine explosion en France

AGENDA

/ 01 Les concepts associés à la PKI Page 12

/ 02 Les atouts d'une PKI Page 18

/ 03 Comment mener un projet PKI ? Page 32

/ 04 Vision du marché de la PKI Page 43

/ 05 Retours d'expérience Page 48

/ 01 Les concepts associés à la PKI

Cryptographie symétrique et asymétrique

/ La **cryptographie symétrique** se base sur une **unique clé** pour les actions de chiffrement

/ La **cryptographie asymétrique** se base sur une **clé publique** et une **clé privée** pour les actions de chiffrement

LA CLÉ PUBLIQUE

/ Pour **chiffrer** les données

/ Pour **vérifier** les signatures

A distribuer à n'importe qui sans crainte !

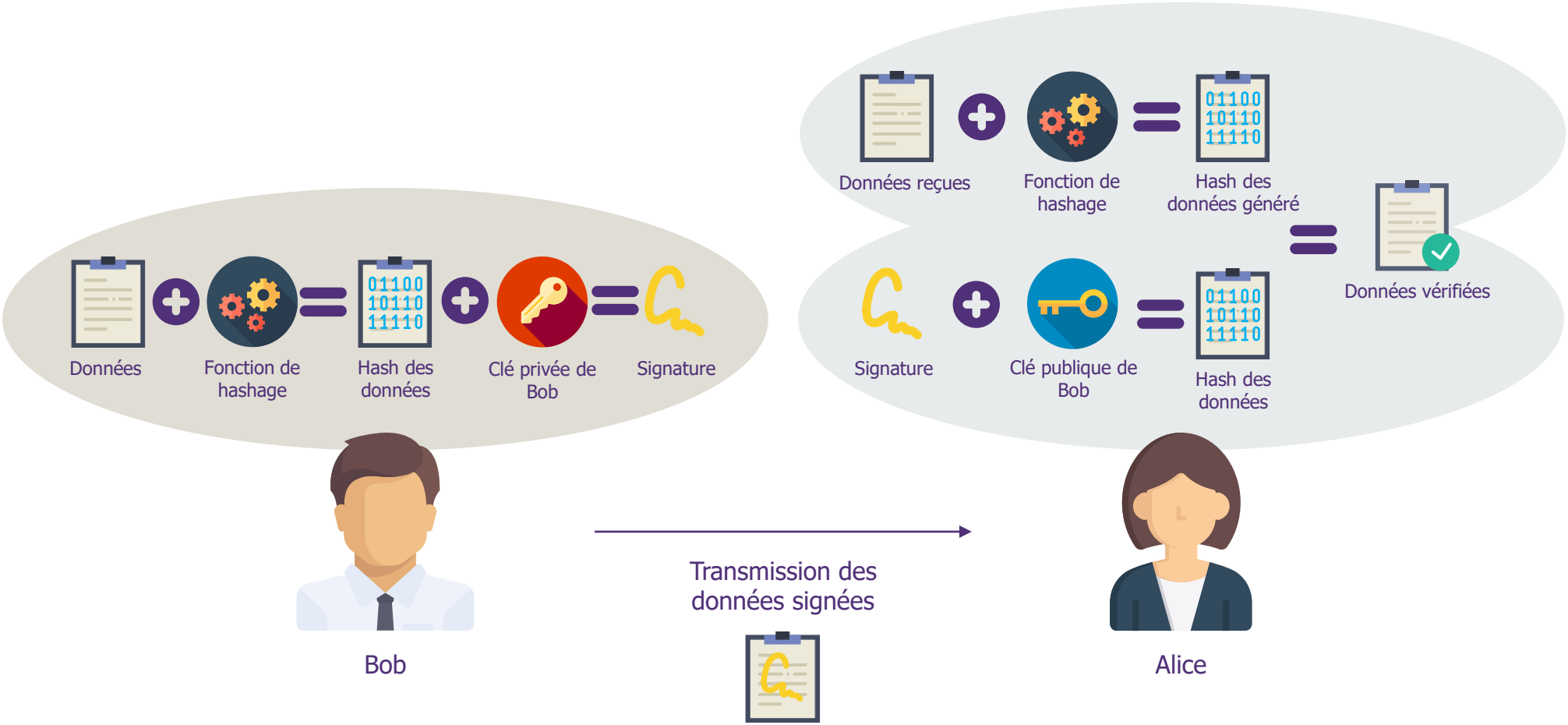
LA CLÉ PRIVÉE

/ Pour **déchiffrer** les données

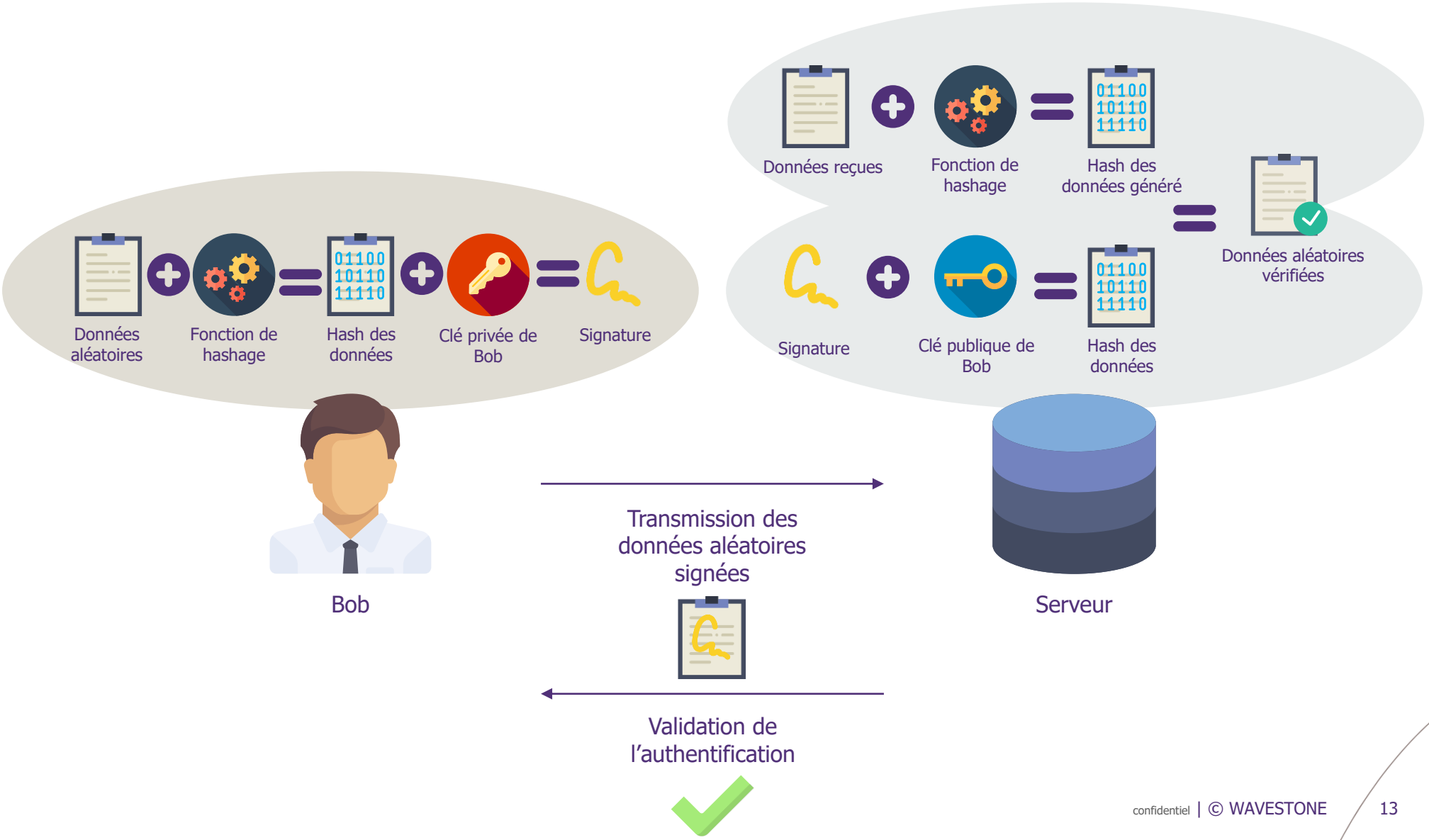
/ Pour **signer** les documents

A conserver secrète par le propriétaire !

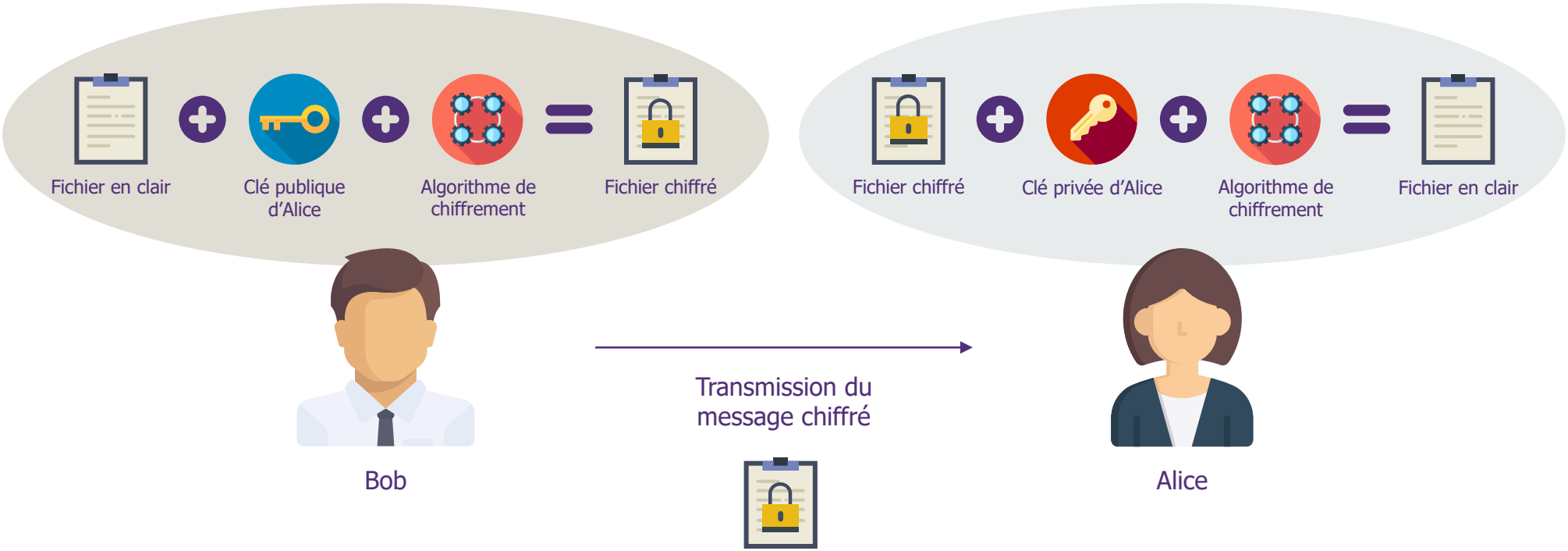
Le fonctionnement de la signature



Le fonctionnement de l'authentification

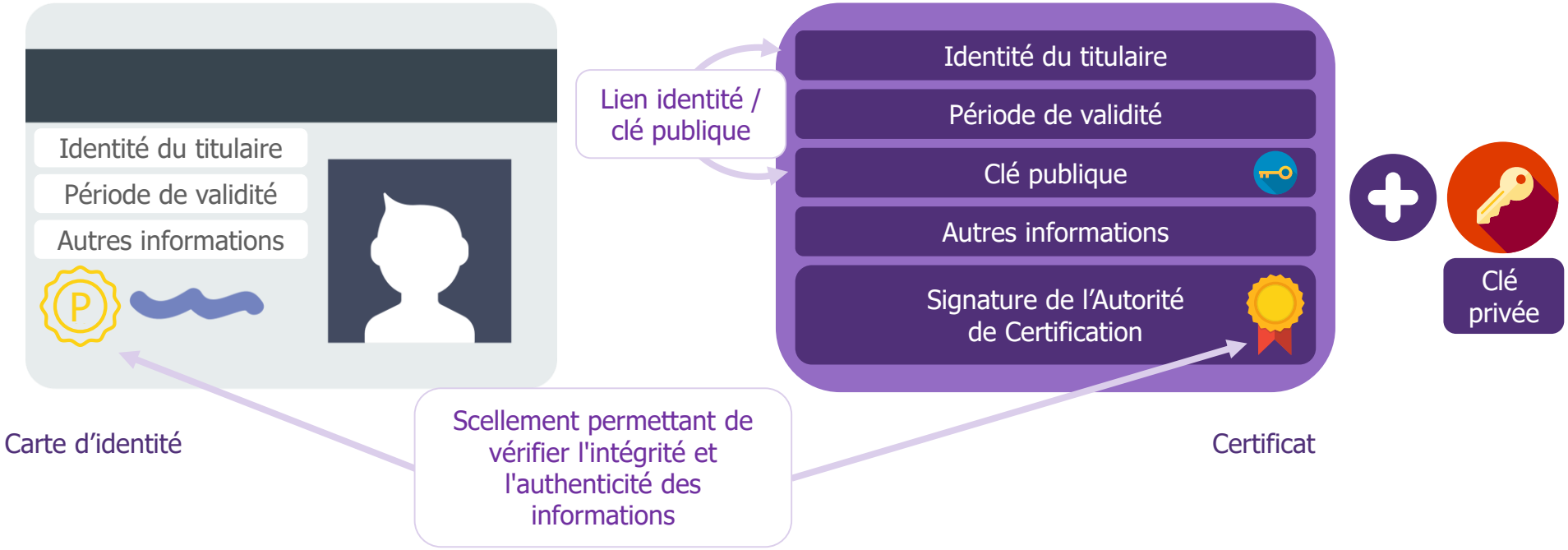


Le fonctionnement du chiffrement



Le certificat électronique (norme X.509)

- Un certificat électronique établit le **lien entre l'identité d'un porteur et sa clé publique** : il s'apparente à une pièce d'identité « électronique »



- Un certificat ne garantit pas les habilitations de son porteur, mais seulement son identité (certifiée par une **Autorité de Certification**), vérifiée lors de l'enregistrement (assuré par une **Autorité d'Enregistrement**)

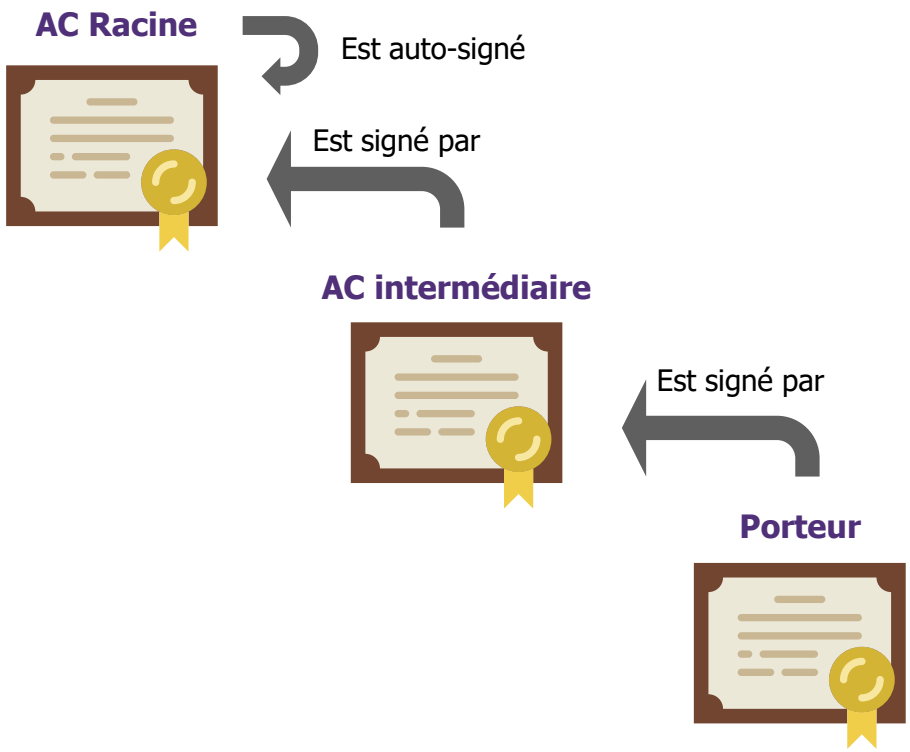
Le certificat ne vaut pas droit !

Garanti du niveau de sécurité de l'IGC

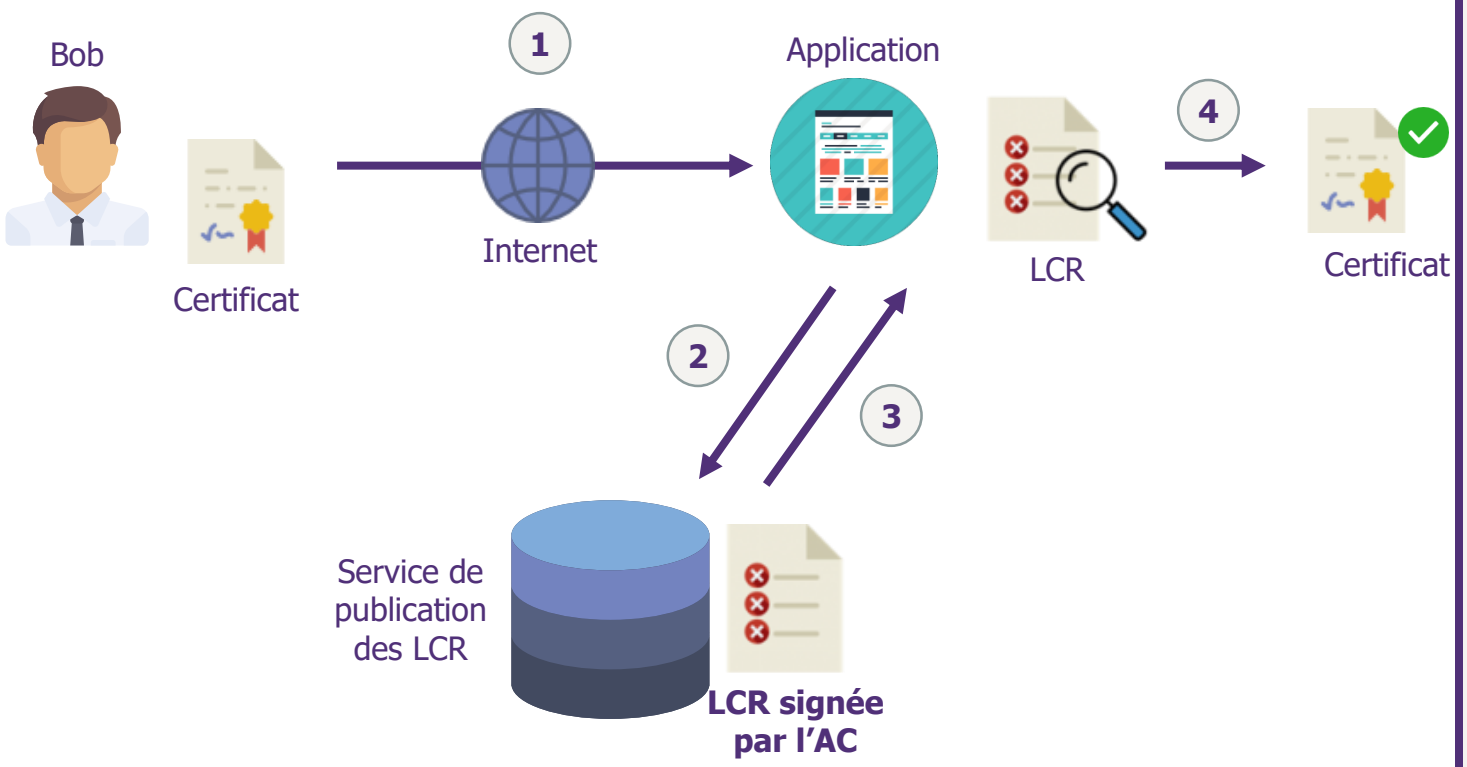
Contrôles à mettre en place côté application

- Nom
- Date de début
- Date de fin
- Vérification de la présence dans la Liste des Certificat Révoqués (LCR)
- Émission par une AC de confiance
- Signature par l'AC
- Usages et usages étendus
- Type de porteur : porteur final ou AC
- Longueur de chaîne de certificats

Hiérarchie de signature mise en place par l'IGC



Garanti du niveau de sécurité dans le cas d'une connexion à une application



1. Bob tente d'accéder à une application et présente son certificat
2. L'application récupère la dernière LCR publiée auprès du service de publication
3. Le service de publication transmets la LCR à l'application
4. L'application vérifie que le N° de série du certificat de Bob ne figure pas

En cas de compromission de la clé privée de Bob, la révocation va permettre d'empêcher l'accès à l'application

Public Key Infrastructure (PKI) ou Infrastructure de Gestion de Clés (IGC)

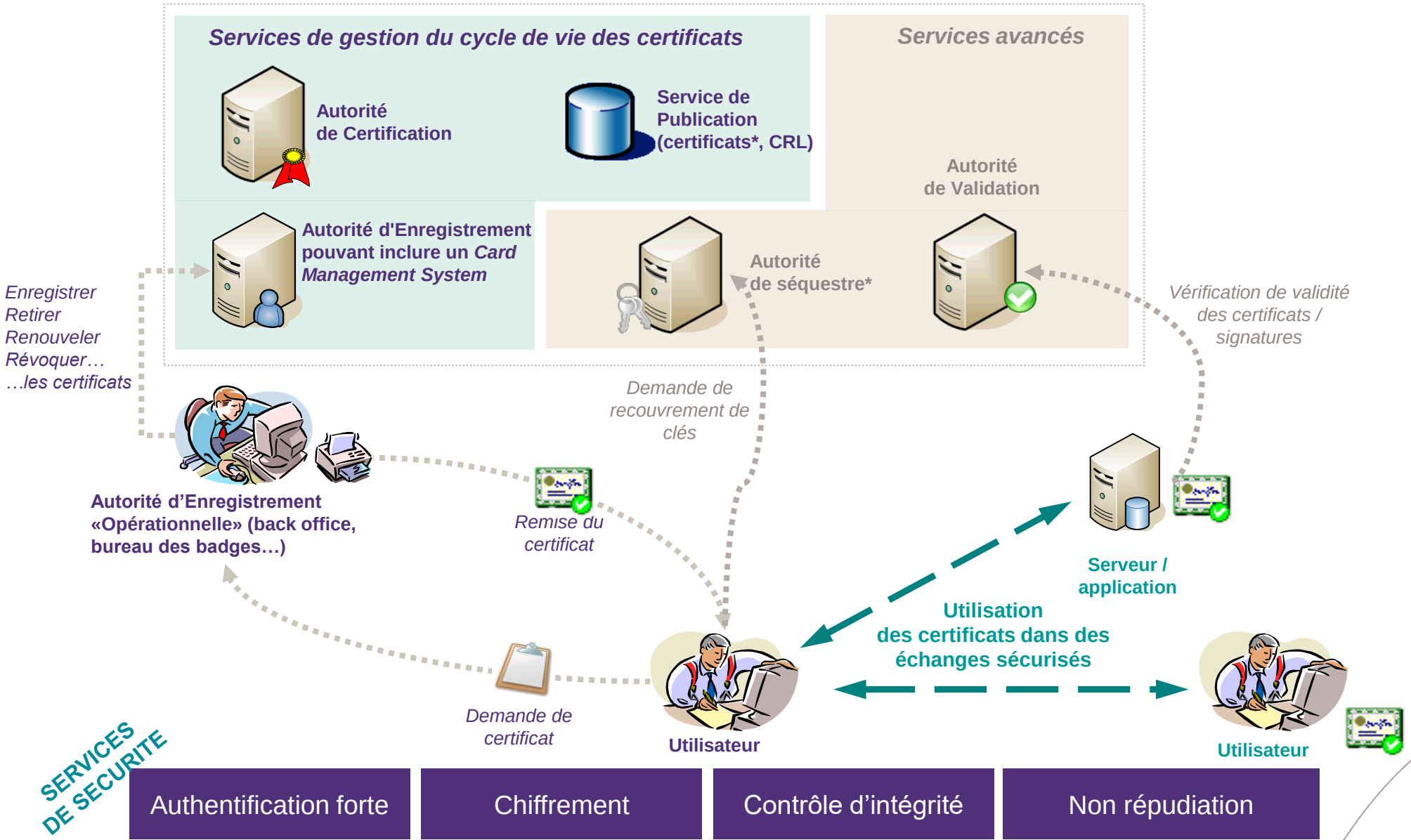
Fonctions de l'IGC		
Briques techniques	**Processus**	**Organisation**
Composants techniques de l'IGC	Gestion au long du cycle de vie garantissant le niveau de sécurité	Répartition des rôles afin de garantir le niveau de sécurité attendu

PKI

« Ensemble de composants, fonctions et procédures dédié à la gestion de clés et de certificats utilisés par des services de sécurité basés sur la cryptographie à clé publique »

Source : Politique de Certification Type - Ministère de l'Économie, des Finances et de l'Industrie

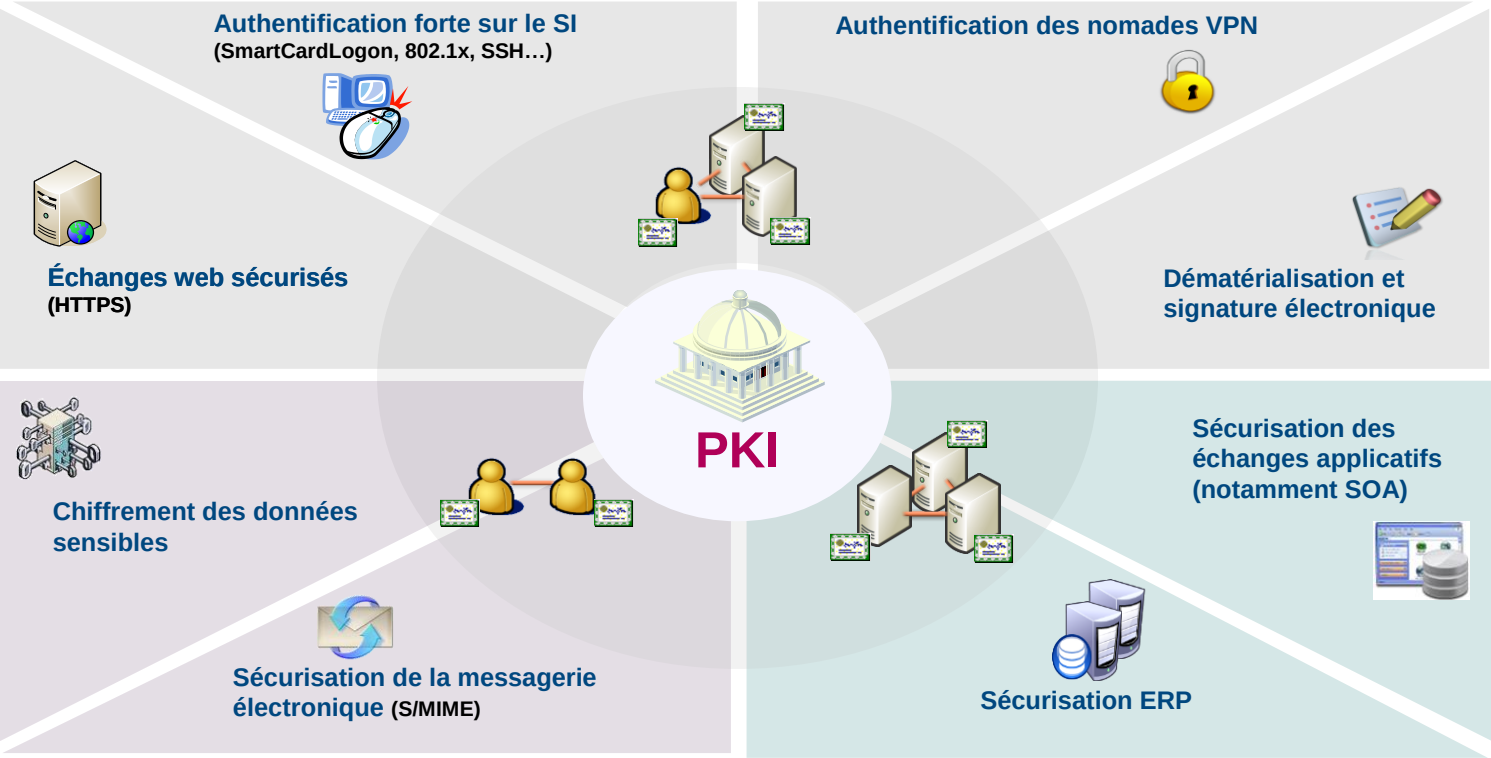
Schéma fonctionnel simplifié d'une PKI



* Uniquement pour des certificats de chiffrement

La PKI : une offre de service pour des projets de sécurisation

/ Les **cas d'usage** des certificats électroniques



Même si tous les domaines ne sont pas encore facilement « PKIsables », les certificats peuvent être intégrés dans un nombre de solutions croissant

/ Le simple **fait de posséder un certificat électronique ne permet pas** de s'authentifier sur une application, de signer électronique des transactions ou de chiffrer un document !

La PKI **contribue** à la mise en œuvre d'usages sécurisés

/ **02**

Les atouts d’une PKI

Introduction

Une solution de sécurité unique et homogène

Une technologie mature

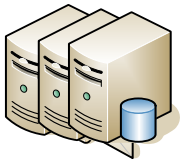
Atouts

Une reconnaissance juridique

Des retours d'expérience significatifs

Une solution de sécurité unique et homogène

/ De **nombreux services de sécurité** offerts

Services	Authentification forte	Chiffrement	Contrôle d'intégrité Non répudiation
Populations	*Utilisateurs (internes ou externes)*	*Applications Composants d'infrastructure* 	*Postes de travail*

/ **Homogénéisation** des procédures

- Rationalisation et formalisation des procédures de gestion des secrets
- A terme pour les utilisateurs internes, un objet de sécurité unique associé à un processus de gestion unique : le **badge SI**

/ Les bénéfices pour les **métiers**

- Plus de gestion des *authentifiants* pour les métiers qui peuvent se concentrer sur les habilitations
- La PKI : **la réponse incontournable pour la signature électronique** nécessaire à la dématérialisation de certains flux

Une technologie mature

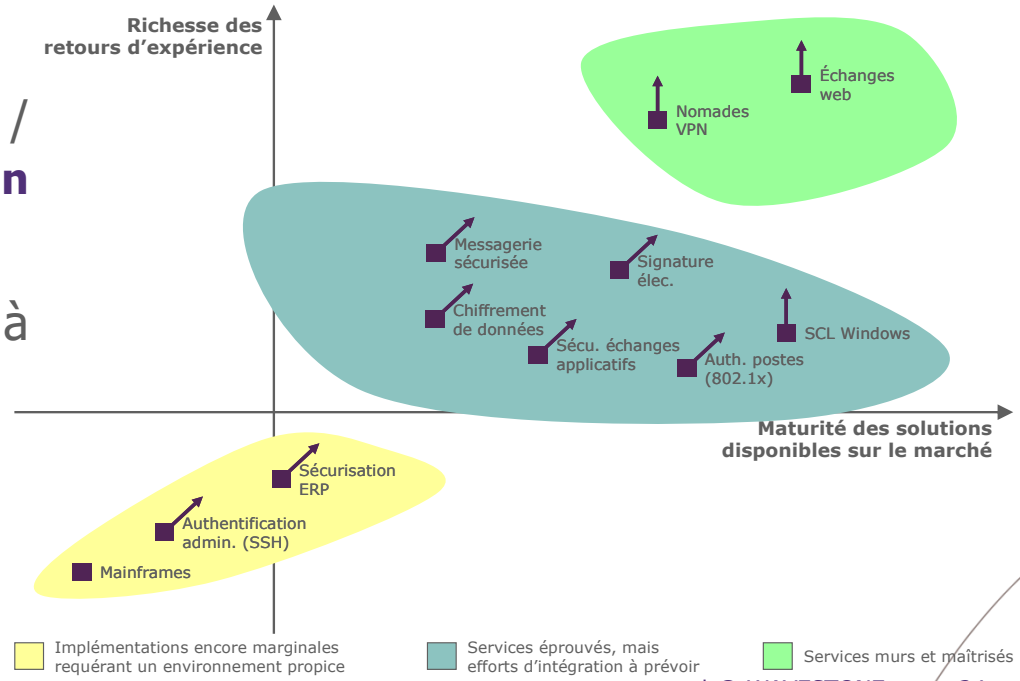
/ Des normes et standards reconnus

- Format des certificats défini dans la norme X509v3 de l'ITU
- **Normes de l'IETF** : Certificat X509 et PKI (RFC 5280), protocoles de sécurisation SSL / TLS (RFC 5246) et S/MIME (RFC 5751), jeton d'horodatage (RFC 3161)…
- **Standards W3C** : XML-DSIG (format de signature électronique), XML-ENC (format de chiffrement)…

Une garantie sur le long terme de l'interopérabilité de la technologie PKI avec les autres composants du SI

/ Reconnaissance par les éditeurs / constructeurs du marché avec **de plus en plus de solutions PKI Ready**

/ Mais des **efforts d'intégration** restent à prévoir pour certains usages



Une reconnaissance juridique

Directive européenne 1999/93/CE : des freins au développement des services de confiance numérique dans un contexte européen

- Différences d'interprétation et niveaux d'exigence hétérogènes dans les déclinaisons nationales
- Différences d'appréciation juridique de la valeur de la signature électronique dans les différents pays de l'UE

A partir du 1er juillet 2016 : application du Règlement européen eIDAS

- Établir des règles et les conditions applicables aux services de confiance au sein de tous les États membre
- Instaurer un cadre juridique autour de la confiance numérique

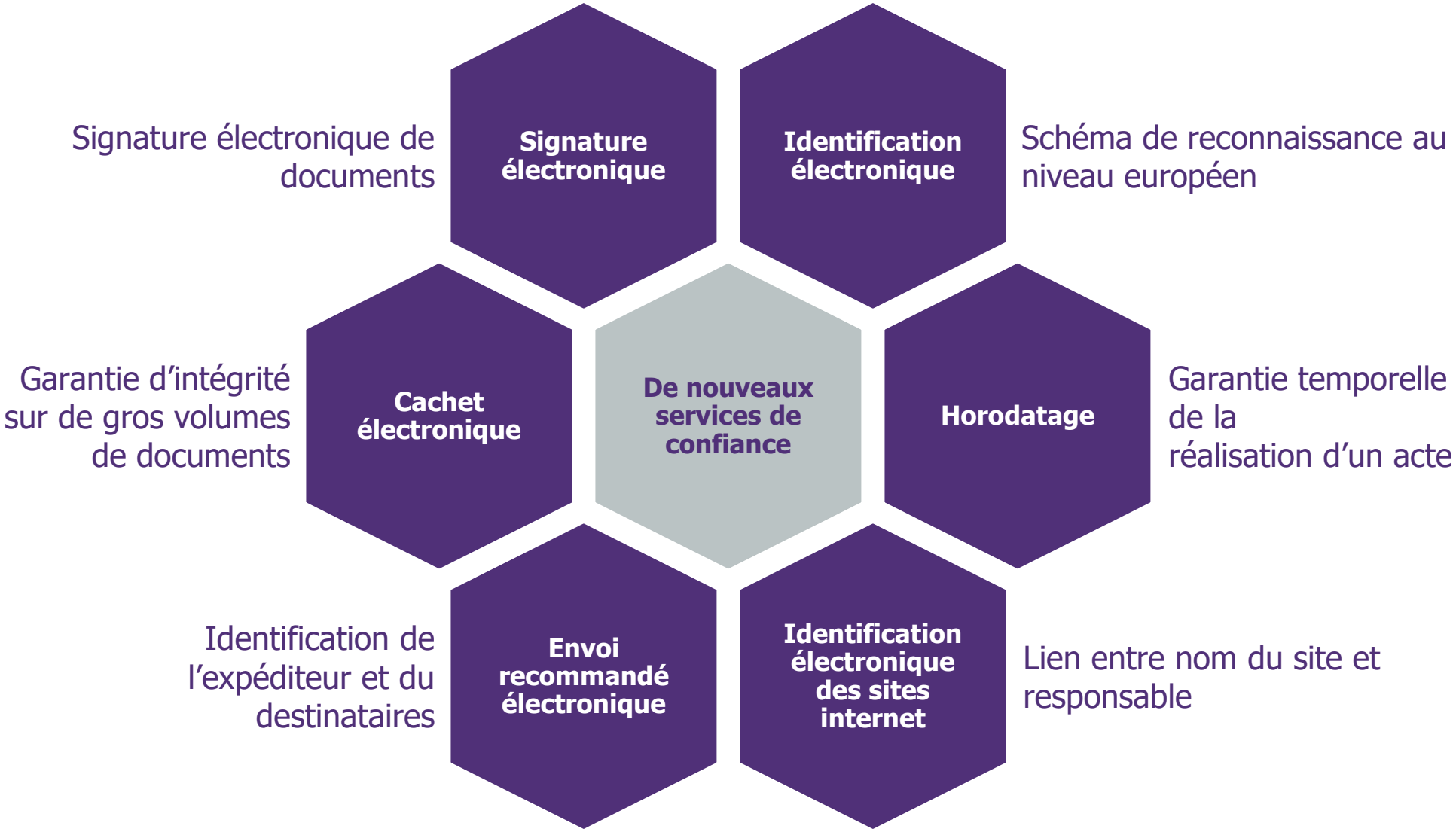
Principaux bénéfices attendus

- **Augmenter la confiance dans l'environnement en ligne pour favoriser le développement économique et social paneuropéen (commerce électronique et secteur public)**

➔ **Une signature aura une valeur identique juridique au sein de l'ensemble de UE**

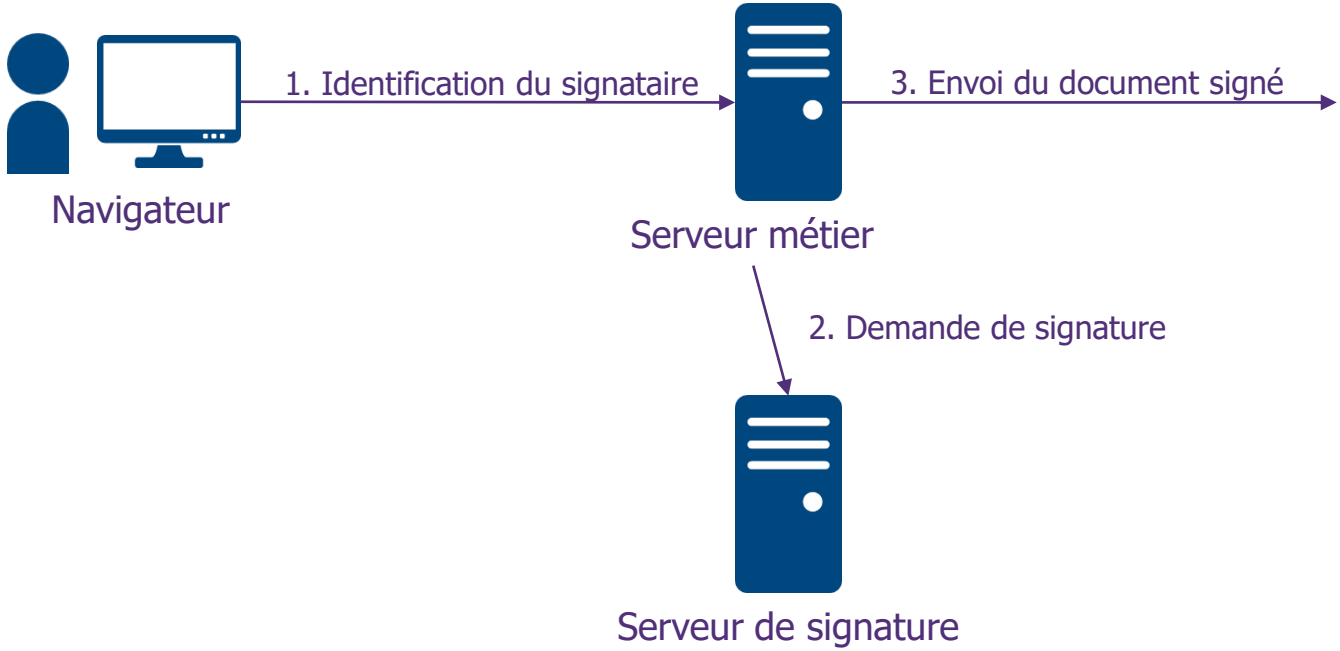
➔ **Les états membres auront l'obligation de reconnaitre les moyens d'identification notifiés par tous les autres états membres**

Le périmètre du règlement européen



Cas d'usage possible : signature simple

Principe :
- Lier un identifiant à un acte et garantir l'intégrité des données
- Identification simple du signataire (nom et prénom a minima)

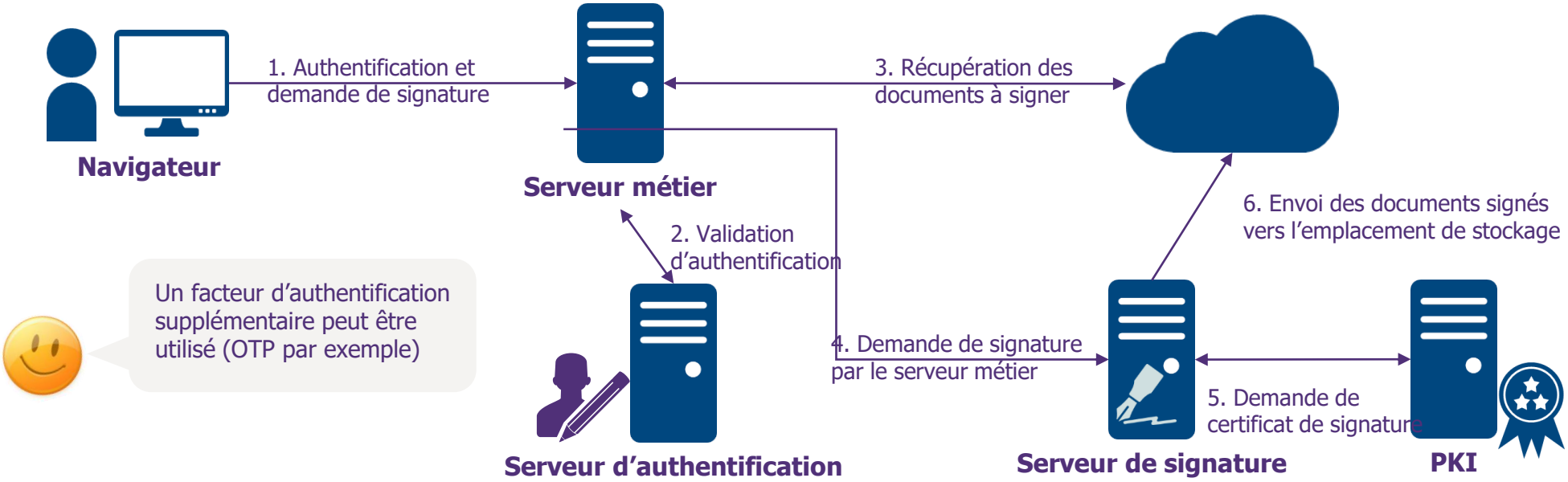


Différents éléments peuvent constituer la preuve d'identité :
- Nom & prénom
- Adresse mail
- Signature manuscrite dessinée à la souris
- Vérification de l'identité par SMS
- Adresse IP
- Logs
- …

Avantages	Inconvénients
• Très simple à mettre en œuvre • Ne nécessite pas d'infrastructure particulière	• Force probante minimale • Utilisation d'un certificat simple, dont la légitimité est à prouver

Cas d'usage possible : signature avancée à l'aide d'un certificat généré à la volée

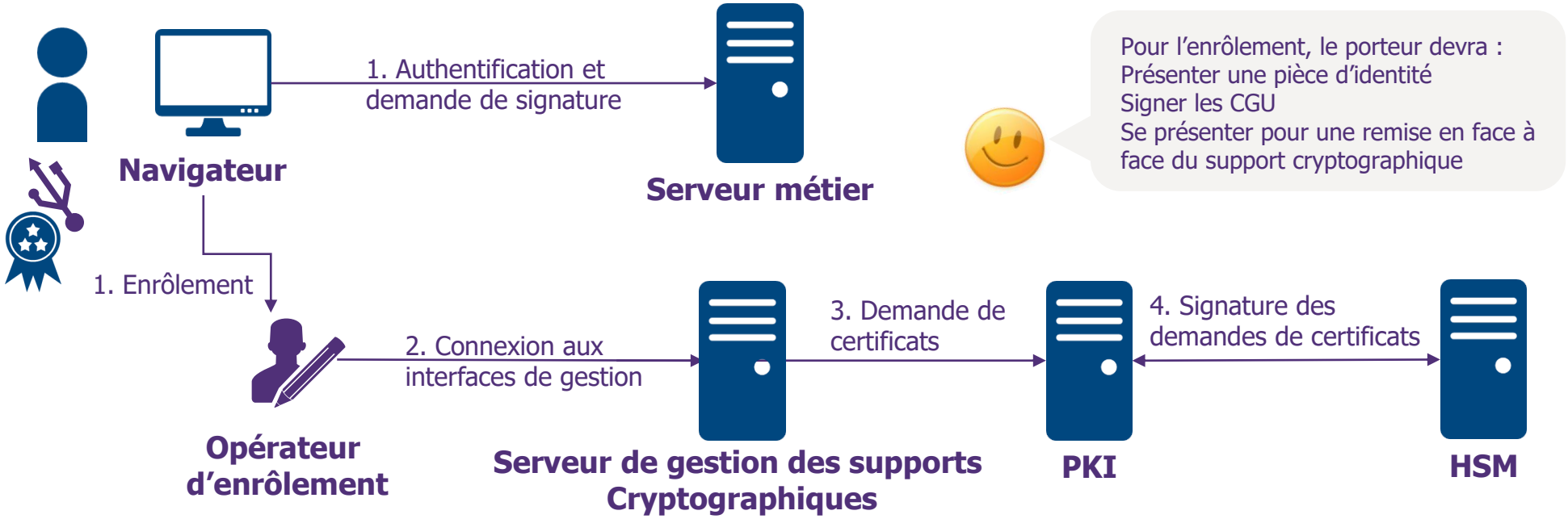
Principe :
- Authentifier le signataire (personne physique)
- Générer, pour chaque transaction, un nouveau certificat à très courte durée de vie



Avantages	Inconvénients
▪ Mise en œuvre assez simple, qui permet l'intégration de la signature électronique dans les workflows métiers ▪ Aucun déploiement particulier auprès du porteur	▪ Nécessité de disposer d'une infrastructure disponible ▪ Horodatage des signatures nécessaire pour vérification a posteriori

Cas d'usage possible : signature qualifiée côté client

Principe :
- Établir un process d'identification préalable à la demande de certificat pour garantir l'identité du porteur
- Déployer un dispositif de création de signature électronique qualifiée avec une remise en face à face

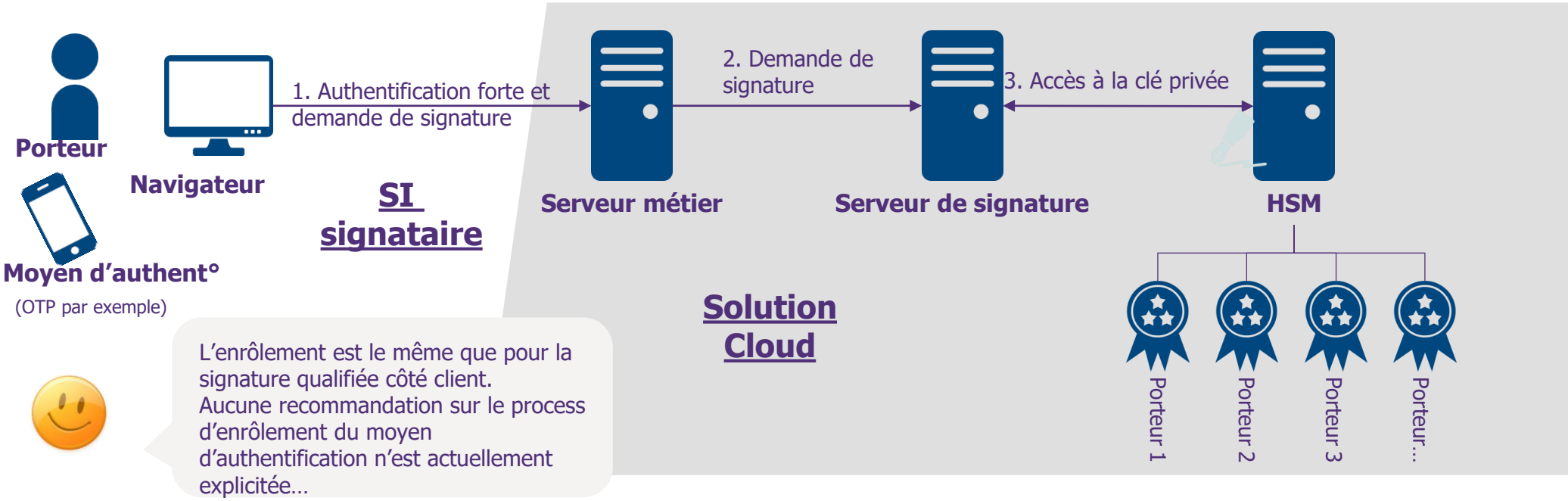


Avantages	Inconvénients
▪ Produire une signature qualifiée ▪ Données d'activation de la clé privée détenues exclusivement par le signataire ▪ Matérialisation du moyen de création des signatures	▪ Déployer et gérer les supports cryptographiques ainsi que le cycle de vie des certificats ▪ Difficultés d'intégration de signature qualifiée dans des flux métiers

Cas d'usage possible : signature qualifiée côté serveur

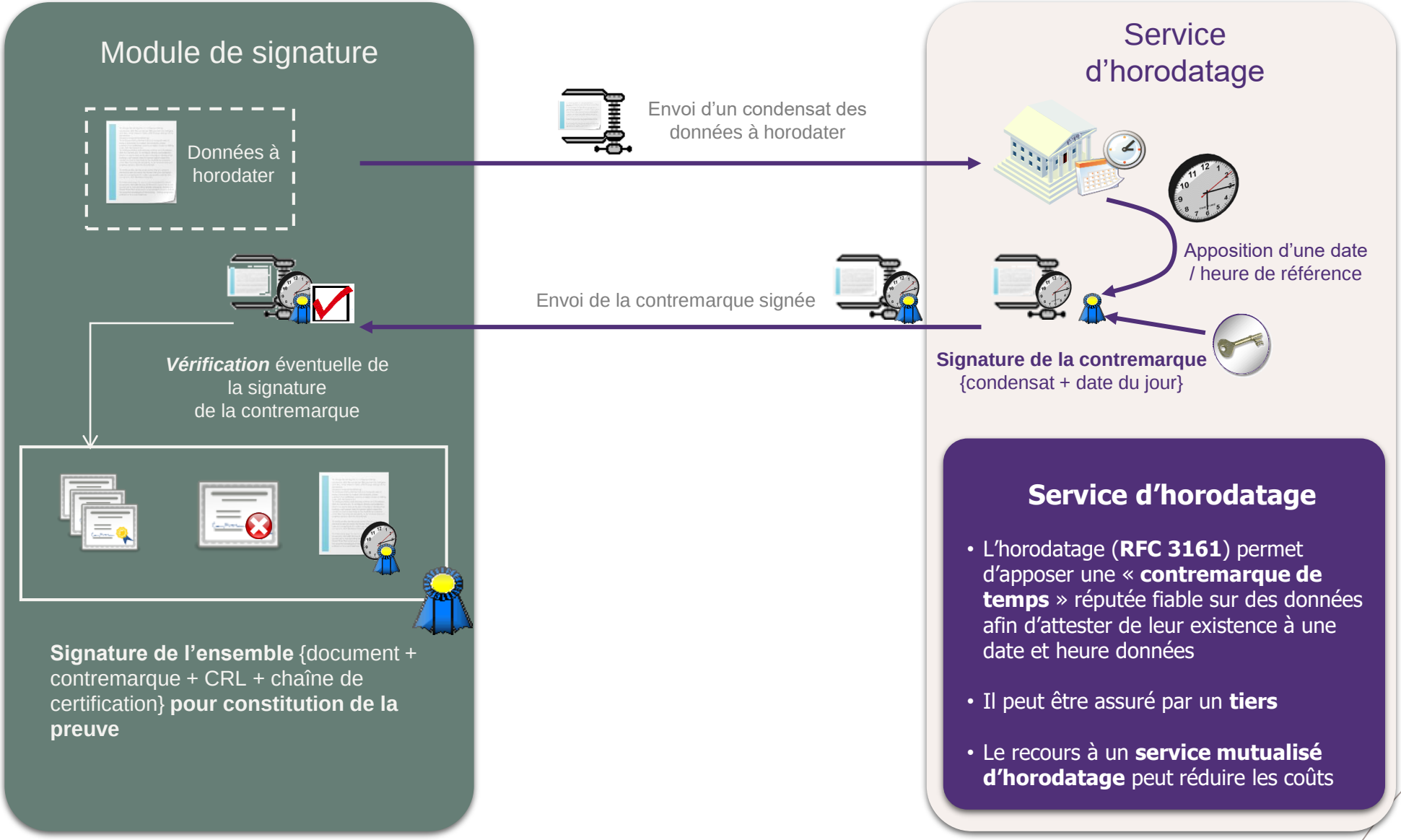
Principe :

- Établir un processus d'identification préalable à la demande de certificat pour garantir l'identité du porteur
- Authentifier **fortement** le porteur et lui donner accès à sa clé de signature



Avantages	Inconvénients
▪ Produire une signature qualifiée ▪ Accès simplifié au certificat de signature du porteur depuis les applications métiers ▪ Évite les coûts de déploiements de support physiques	▪ Maintenir les processus de gestion des cycles de vie des certifications ▪ Prévoir un volume suffisant au niveau du HSM pour assurer les performances du service

Focus sur l'horodatage



Service d'horodatage

- L'horodatage (**RFC 3161**) permet d'apposer une « **contremarque de temps** » réputée fiable sur des données afin d'attester de leur existence à une date et heure données
- Il peut être assuré par un **tiers**
- Le recours à un **service mutualisé d'horodatage** peut réduire les coûts

Des retours d'expériences dans les entreprises

	Populations	Usages			Supports
		Auth. Forte	Chiffrement	Signature	
SOCIETE GENERALE GROUPE	Porteurs internes	✓		✓	Carte à puce
	Applications	✓			Certificat logiciel ou HSM*
CRÉDIT AGRICOLE / CREDIT LYONNAIS	Porteurs internes	✓	✓	✓	Carte à puce
	Porteurs externes	✓		✓	Certificat logiciel
	Applications	✓			Certificat logiciel ou HSM
BANQUE DE FRANCE	Porteurs internes	✓	✓	✓	Carte à puce ou logiciel
	Porteurs externes		✓	✓	Carte à puce ou logiciel
	Applications	✓		✓	Certificat logiciel ou HSM
BNP PARIBAS	Porteurs internes	✓	✓	✓	Certificat logiciel
	Applications	✓			Certificat logiciel ou HSM
L'ORÉAL	Porteurs internes	✓	✓	✓	Carte à puce
	Applications	✓		✓	Certificat logiciel ou HSM
TIGF	Porteurs internes	✓	✓	✓	Carte à puce
	Applications	✓			Certificat logiciel ou HSM

** Hardware Security Module : boîtier cryptographique pour application*

Projets en cours

… suite …

	Populations	Usages			Supports
		Auth. Forte	Chiffrement	Signature	
TOTAL	Porteurs internes	✓	✓	✓	Carte à puce
	Porteurs externes	✓		✓	Certificat logiciel
	Serveurs	✓		✓	Certificat logiciel ou HSM
	Postes de travail	✓			Certificat logiciel
AREVA	Porteurs internes	✓	✓	✓	Carte à puce
	Serveurs	✓			Certificat logiciel ou HSM
EDF	Porteurs internes	✓			Carte à puce
	Porteurs externes	✓			Carte à puce
RENAULT	Porteurs internes	✓	✓	✓	Carte à puce
	Porteurs externes	✓			Certificat logiciel
	Serveurs	✓			Certificat logiciel ou HSM
EADS	Porteurs internes	✓	✓	✓	Carte à puce
	Porteurs externes	✓	✓		Certificat logiciel
	Serveurs	✓	✓	✓	Certificat logiciel ou HSM
AIR FRANCE	Porteurs internes	✓		✓	Carte à puce
CNP	Serveurs	✓			Certificat logiciel ou HSM

… et dans les administrations

- Historiquement, précurseur du marché de la certification avec le lancement de Télé-TV@ et la création associée des Autorités de Certifications commerciales

- Multiplication des PKI au sein des grandes administrations centrales (ANPE, MINEFI, Ministère de la Santé, etc.), notamment poussée par le RGS (Référentiel Général de Sécurité) promu par la DGME (Direction Générale de la Modernisation de l'État)/ le SGMAP (secrétariat général pour la modernisation de l'action publique)

- Une forte promotion de la dématérialisation avec utilisation de la signature électronique
  - Pour les échanges C to A : Télé-IR → Plus de 7 millions d'utilisateurs
  - Pour les échanges B to A : Télé-TV@, Téléc@rtegrise, net-entreprises.fr (déclarations sociales), achatpublic.com, marches-publics.gouv.fr → Quelques centaines de milliers d'utilisateurs

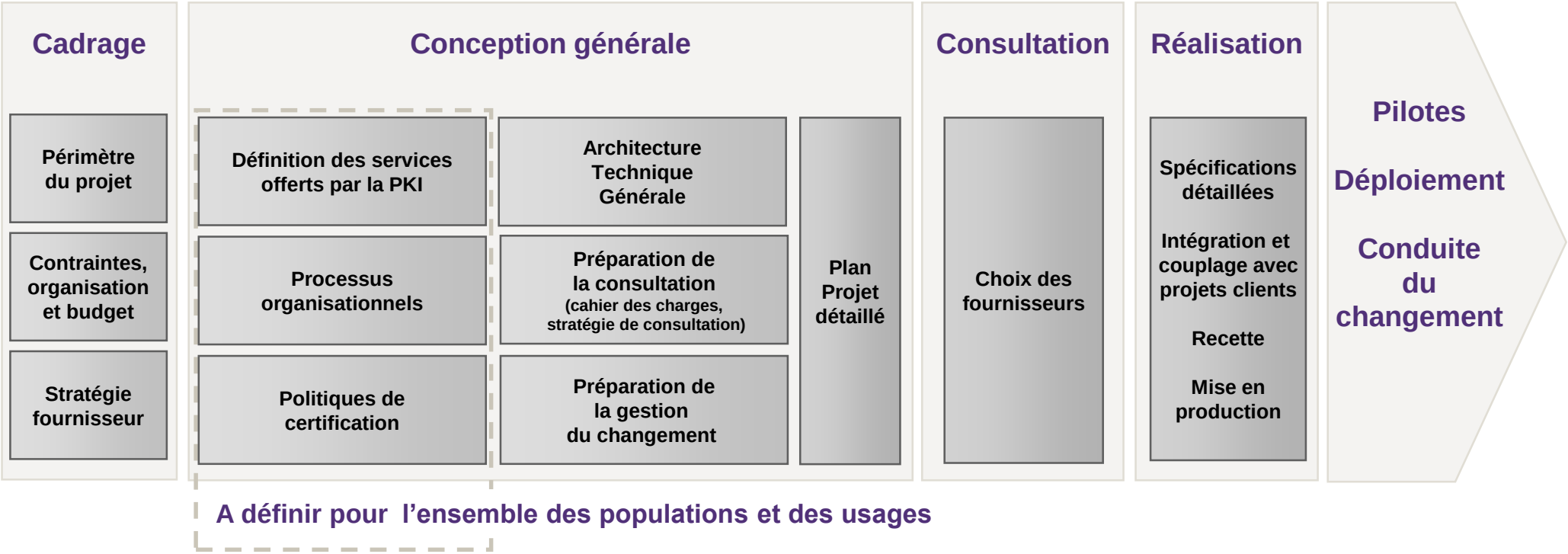
	Populations	Usages			Supports
		Auth. Forte	Chiffrement	Signature	
	Porteurs internes	✓	✓	✓	Carte à puce ou logiciel
	Porteurs externes		✓	✓	Certificat logiciel
	Smartphone	✓			Certificat logiciel
	Applications	✓		✓	Certificat logiciel
	Serveurs				Certificat logiciel ou HSM

Projets en cours

/ **03**

Comment mener un projet PKI ?

Un projet PKI : des grands chantiers organisationnels et techniques



La phase de conception générale : la **phase stratégique** d'un projet PKI
Objectif : gagner la maîtrise du projet et notamment des fournisseurs (planning et coûts)

Les principaux enjeux

/ Cadrer le **périmètre** du projet

- En termes d'usages : une PKI, pour quoi faire ?
- En termes de contraintes : existe-t-il des contraintes règlementaires ?
- En termes de planning : arbitrer les besoins et privilégier une approche évolutive

Adopter une démarche de mise en place progressive en ciblant d'abord les usages à fort enjeu : «cibler loin et jalonner court»

/ Comprendre le SI **existant** et évaluer les **impacts** et **évolutions** amenés par le projet

- Identifier les impacts de l'intégration des certificats et des supports matériels dans le SI
- Maîtriser les impacts sur les solutions de sécurité existantes

/ Choisir la **solution technique**

- Choisir le support des certificats → La tendance : le support matériel pour les utilisateurs internes mais attention aux contraintes de mobilité sur des postes non maîtrisés ou à l'utilisation de dispositifs mobiles !
- Choisir une stratégie fournisseur

Internalisation	Externalisation
Mettre en œuvre et exploiter les composants techniques de la PKI en s'appuyant sur des **solutions logicielles à intégrer**	Utiliser les services d'un **Opérateur de Certification** fournissant et exploitant les briques techniques de la PKI (service opéré)

Aucune approche privilégiée a priori : à considérer en fonction du contexte

/ Sans oublier les aspects liés à la **mise en place de l'organisation et des procédures associées…**

- Valider la qualité du provisioning et définir l'ensemble des processus (y compris exceptionnels)
- Traiter la gestion du changement auprès des utilisateurs (communication/formation)
- Valider la capacité de montée en charge de la PKI sur les plans techniques et organisationnels
- Travailler de concert avec les juristes

/ …et leur **maintien** dans le temps

Choisir une stratégie fournisseur : internalisation ou externalisation ?

/ Internalisation ou externalisation : la problématique…

- Possibilité d'internaliser/d'externaliser tout ou partie de l'infrastructure : AC, AE, Back-Office (ex. : hébergement des AC, personnalisation des cartes à puce, support téléphonique)

/ Comparaison des deux approches

Internalisation

Maîtrise de l'**exploitation technique**

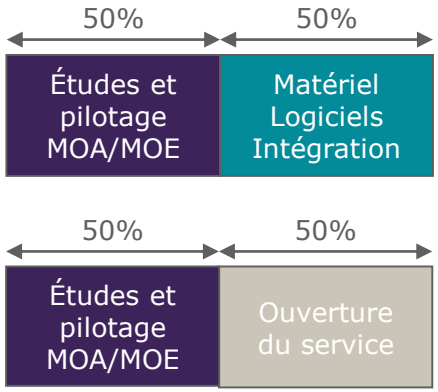
Meilleure adaptation aux besoins d'**exploitation fonctionnelle** (ex. : *workflow* de facturation)

Externalisation

Maîtrise des **coûts** et des **délais** par mutualisation des moyens (physiques, techniques et organisationnels)

Service clé en main, d'où **limitation des risques projet**

Répartition des coûts



/ Les éléments de décision

- Analyser le contexte de l'entreprise (maîtrise de la solution, compétences, etc.)
- Avoir une connaissance pointue des solutions disponibles sur le marché
- Se prémunir de la fragilité des acteurs en garantissant la réversibilité des solutions
  - Possession des HSM, définition d'une couche d'abstraction entre l'AC et l'AE techniques

Les deux approches sont viables, le choix relève le plus souvent du contexte interne et de la stratégie de l'entreprise

Identifier les impacts et l'intégration des certificats dans le SI

/ Impact sur les postes des utilisateurs

› Nécessité d'installer des logiciels sur les postes de travail :

» la chaîne de certification,

» les pilotes des supports matériels (si utilisés),

» des logiciels spécifiques (pour faire du chiffrement, de la signature électronique…)

Impact potentiellement faible sur des postes maîtrisés car possibilité de télédistribuer les logiciels

/ Impact sur les applications

› Assistance auprès des Métiers pour l'intégration des certificats

» Vente du projet auprès des Maîtrises d'Ouvrage et des Maîtrises d'Œuvre

» Assistance à l'intégration des certificats dans les applications

» Constitution de guides d'intégration dans les applications « classiques »

Impact plus ou moins important en fonction des applications

Maitriser les impacts sur les solutions de sécurité existantes

- Gérer l'interaction avec les **annuaires**
  - Utilisations possibles des annuaires
    - Publier les listes des certificats révoqués et les certificats de chiffrement
    - Utiliser les données existantes pour faciliter l'enregistrement des utilisateurs
  - Identification des adhérences éventuelles entre le nommage des certificats et l'arborescence de l'annuaire
- Avoir un **identifiant unique**
  - Impact fort si « l'identifiant unique » est hétérogène au sein de l'entreprise
- Analyser l'interaction avec ***l'Identity Management***
  - Les produits d'IDM gèrent les certificats et peuvent s'intégrer avec la PKI (dans ce cas ils peuvent constituer une Autorité d'Enregistrement technique)
- Définir les opportunités d'intégration des certificats dans les solutions de **SSO**
  - La PKI ne fournit pas une solution de SSO mais fournit un composant d'authentification unique

Choisir le support des certificats : critères de décision (1/2)

/ Problématique : où stocker les clés privées et certificats ?

› Magasin de certificats logiciel ou support matériel (carte/clé à puce, *Hardware Security Module*, *Trusted Platform Module*) ?

Niveau de criticité des applications à sécuriser

- Un support matériel offre une sécurisation accrue des clés privées
- La signature électronique peut imposer l'utilisation d'un support matériel

Niveau de maîtrise de la sécurité des postes de travail et des serveurs

- Le magasin de certificats logiciel est le support préférentiel pour la sécurisation des applications (serveur web etc.) dont le processus d'exploitation est maîtrisé
- Pour des postes de travail et/ou des applications non maîtrisés, s'orienter plutôt vers un support matériel

Impact du déploiement des supports matériels sur les machines cibles

- Installation des pilotes et du *middleware*

Coûts de fonctionnement

- Un support matériel augmente les coûts de fonctionnement
- ~15€/porteur/an pour cartes/clés, HSM plusieurs k€

Mobilité

- Un support matériel peut favoriser la mobilité des porteurs

Choisir le support des certificats : critères de décision (2/2)

Support matériel : clé ou carte à puce ?

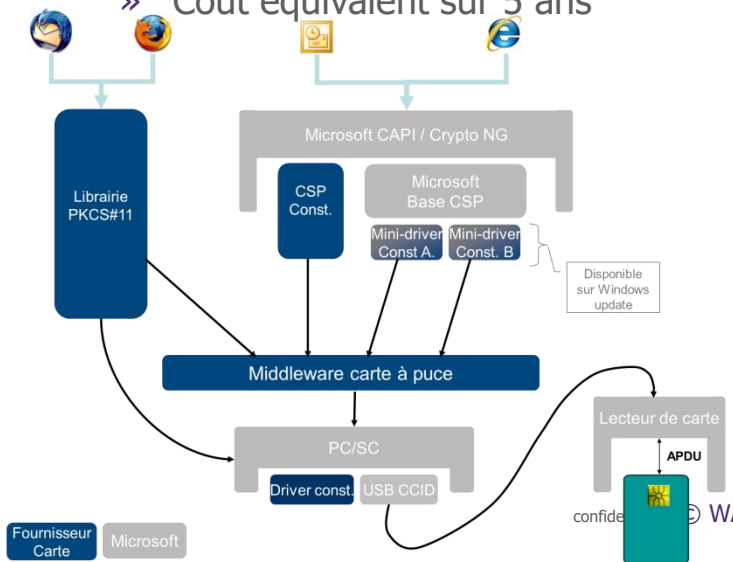
/ Environnements systèmes supportés
  - » En général environnements Microsoft mais pas uniquement

/ Interopérabilité entre les composants carte, lecteur et middleware
  - › De nombreux fournisseurs de cartes/clés à puce et lecteurs sur le marché (ex. : ActivIdentity, Gemalto, Safenet, Oberthur, Sagem, Utimaco)
  - › Des fonctionnalités différentiantes des middleware / carte
    - » Gestion du PIN : PIN Caching, Multi PIN, Déblocage, Biométrie Match On Card
    - » Capacité
    - » Niveau de sécurité (FIPS, EAL, SSCD, etc.)
    - » Performances
    - » Possibilité de déploiement sur postes non maîtrisés : compatibilité MS BASE CSP, support USB PC/SC

› Le choix du lecteur n'est pas neutre
  - » Ergonomie notamment en cas de mobilité
  - » Interopérabilité

› Inclusion de technologies spécifiques
  - » Puce(s), bande magnétique, antenne radio
  - » Technologie Java Card, ou OS spécifique (.Net)

› Coûts
  - » Les clés à puce USB ont un coût d'acquisition inférieur au couple carte / lecteur mais avec une durée de vie plus courte
  - » Coût équivalent sur 5 ans



Industrialiser la production du badge unique

/ Des délais de préparation des corps de cartes « badge unique »

› Intégration de multiples technologies « à la demande »

/ Des contraintes industrielles qui impactent la qualité finale du visuel

› Déformation de la surface : puce à contact et puce sans contact

→ Prendre en compte l'emplacement des puces dans le corps de carte

› Charte graphique : faire valider l'impact de l'implantation de la puce à contacts sur le visuel

→ Prendre en compte le délai de validation par les entités Communication ou Image de marque

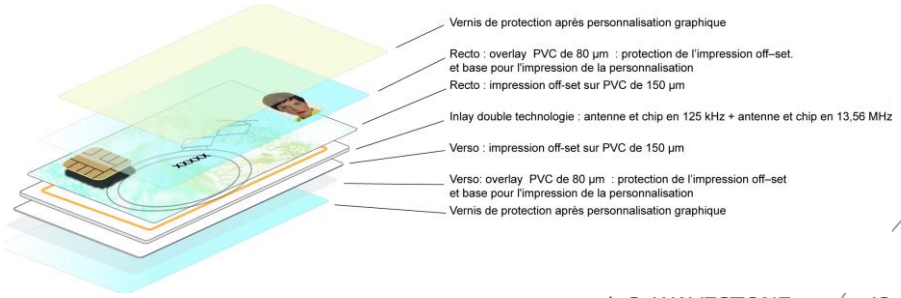
/ Des contraintes liées à la personnalisation qui contraignent la composition du visuel et les choix technologiques

› Technologie d'impression : risques sur la qualité graphique

› Capacité d'encodage (technologies prises en charge)

→ Impact faible sur les coûts d'acquisition

→ Impact fort sur les coûts récurrents de personnalisation



La définition de processus simples et maintenables dans le temps

/ La distribution initiale : une véritable conduite du changement

- Plan de communication
- Organisation du déploiement par vague
- Support rapproché et renforcé
- Prise en compte des populations spécifiques : VIP, nomades

/ Des processus récurrents maintenables

Besoin utilisateur	Processus PKI /Carte
Besoin d'un certificat	Souscription d'un utilisateur
Oubli du mot de passe du token (ou carte à puce)	Réinitialisation du PIN
Oubli du token (ou carte à puce)	Génération d'une carte à puce de secours (ou token USB)
Perte du token (ou carte à puce)	Re-génération d'une carte à puce (ou token) après perte
Changement des données utilisateur	Modification des données utilisateur
Plus de besoin du certificat	Révocation du certificat
Recouvrement de documents chiffrés (suite à la perte de la clé)	Recouvrement de la clé de chiffrement
Expiration du certificat	Renouvellement du certificat
Besoin d'un nouveau certificat	Ajout d'un certificat

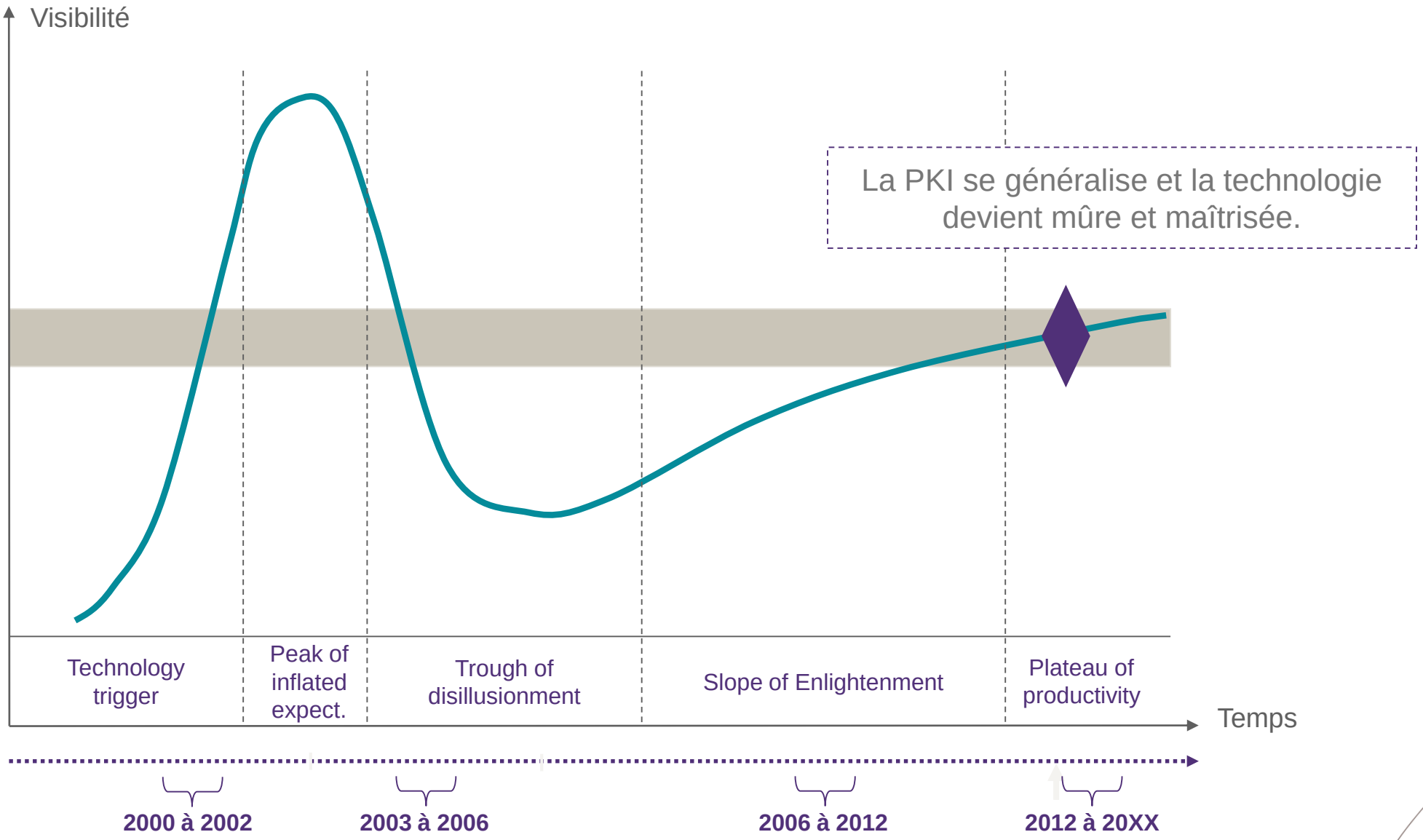
Autres points d'attention particuliers

- Qualité du lien avec l'IDM et qualité des **processus exceptionnels**
  - L'intégration dans les processus d'Identity Management est essentielle (processus de mouvement de personnes en particulier)
  - Définition des processus exceptionnels (perte, vol, oubli…)
- **Communication et formation** auprès des utilisateurs et des métiers
  - Obtenir l'adhésion des acteurs au projet
  - Gérer le changement
  - Maintenir le niveau de sécurité global
- **Capacité de montée en charge** de la solution dans le cadre des différents jalons de mise en œuvre d'une PKI globale
  - Entité organisationnelle (Back Office)
  - Infrastructure technique
- Travailler de concert avec les **juristes**
  - Rédaction des contrats et des conventions de services
  - Validation éventuelle des Politiques de Certification

/ **04**

Vision du marché de la PKI

La vision Wavestone



Depuis 2006, un nouvel engouement pour la PKI

/ **3 moteurs** principaux identifiés

1

Les programmes IAM

Rationalisation de la gestion des identifiants, des droits d'accès et des processus de *provisionning* favorisant le déploiement de certificats électroniques, notamment sur des badges SI
Convergence des moyens d'accès physiques et d'accès logiques au sein d'un même support, la carte à puce : des premiers projets Badge Unique

2

L'essor de la signature électronique

Dématérialisation de processus métier nécessitant un service de non-répudiation

3

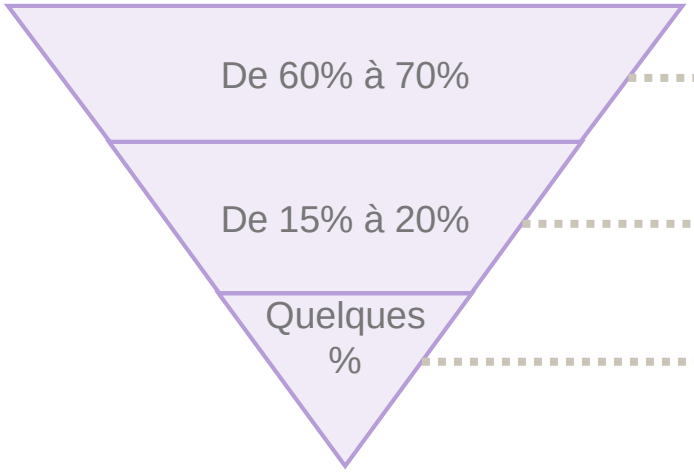
La sécurisation des infrastructures réseaux

Authentification du poste de travail au réseau local (802.1x), sécurisation des couches réseaux inter-entreprises ou intra-entreprise (IPSec…)

La technologie PKI chez les Grands Comptes

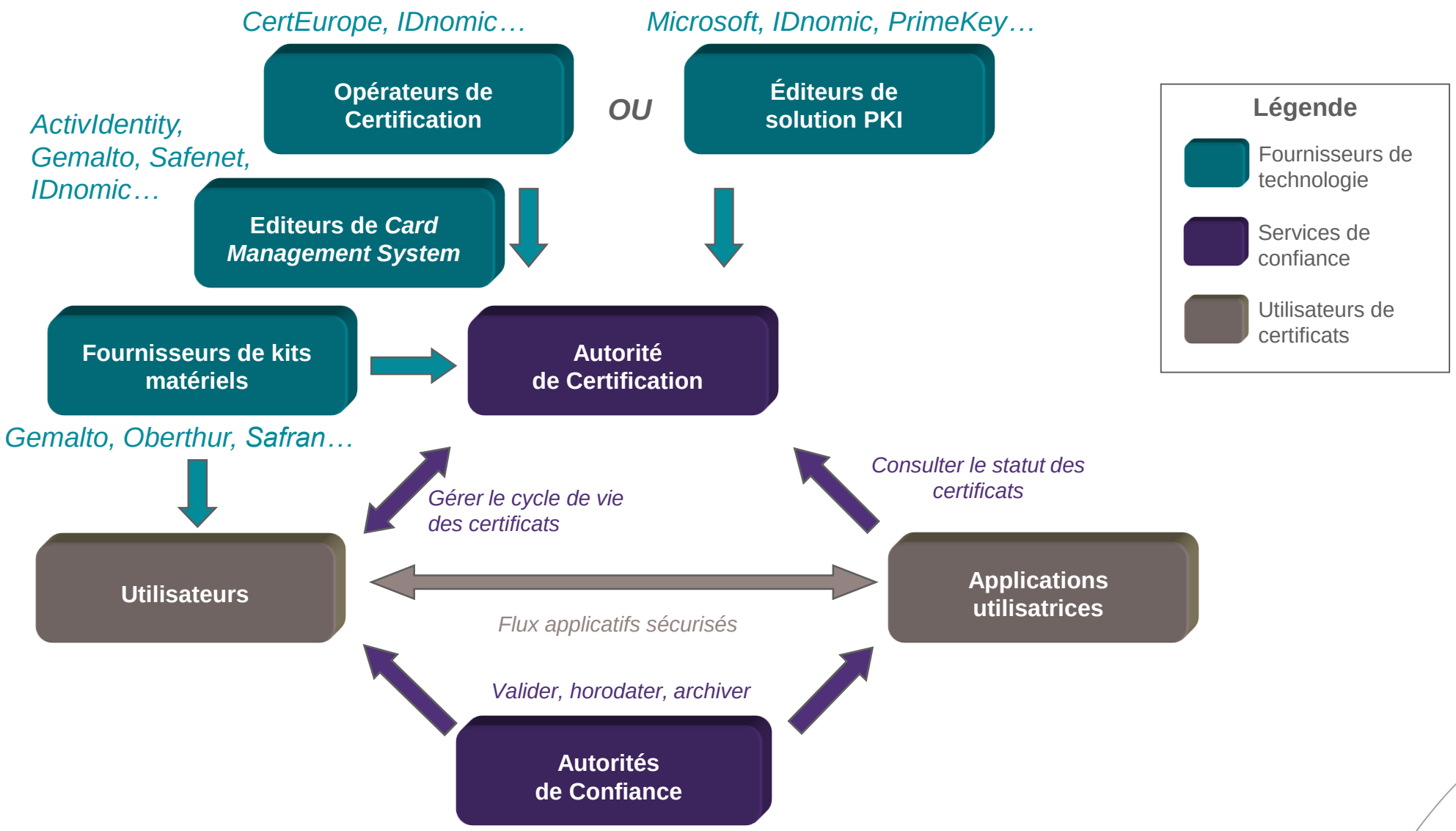
- Tous les Grands Comptes utilisent des certificats électroniques (par exemple, certificats SSL pour les portails web)
- « Posséder une PKI interne » est une règle qui tend à se généraliser, mais son déploiement à grande échelle pour ses utilisateurs internes reste peu courant

Panorama sur les 100 plus Grands Comptes français



- De 60% à 70% → Possèdent une PKI interne
- De 15% à 20% → Délivrent des cartes à puce aux collaborateurs internes
- Quelques % → Déploient des cartes à puce aux collaborateurs internes à grande échelle (+ de 25 % de la population cible)

Les acteurs du marché



Bonnes pratiques et synthèse

Définir le niveau de sécurité cible

/ Référentiel Général de Sécurité : RGS ?

- fixe les règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique
- Travail conjoint de la ANSSI et SGMAP
- Niveau de sécurité: *, ** ou *** (processus, disponibilité, vérification des identités, technicité, etc.)
- Signature qualifiée: niveau *** requis **(pas de mutualisation AC signature/authentification)**

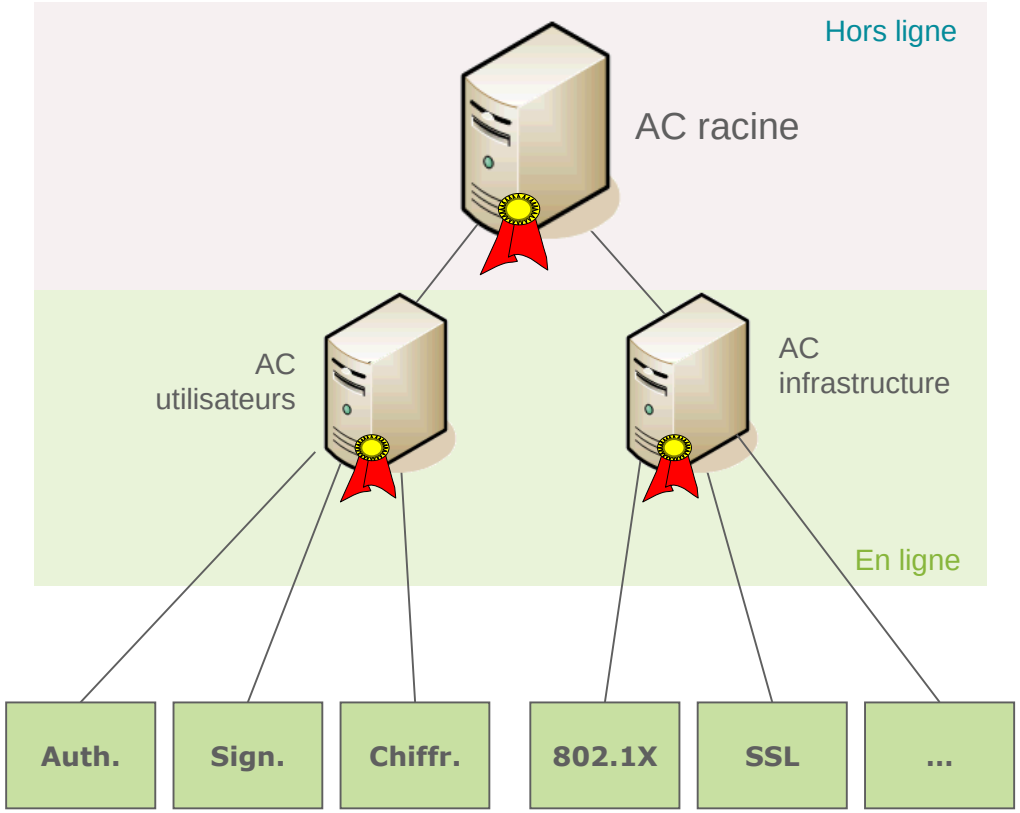
/ Référentiel de bonnes pratiques

Niveau de sécurité	Risque d'usurpation d'identité	Critères techniques et fonctionnels applicables selon le niveau de sécurité
***	**Très fort**	/ Face à face physique avec le porteur / Vérification approfondie de l'identité / Signature électronique de toutes les demandes liés au cycle de vie
**	**Fort**	/ Sauvegarde hors site / Algorithmes à utiliser et taille des clés / Partage des secrets pour la clés privée
*	**Moyen**	/ Qualification requise / Standard du module cryptographique de l'AC

Architecture de l'autorité de certification flexible

Hiérarchiser l'autorité de certification

- **Par type de population** (porteur physique, porteur matériel…)
- **Éviter un découpage par organisation** (entités/filiales)
  - Non nécessairement pérenne dans le temps (changement de nom, fusion, revente de filiale, etc.)
  - Nécessite potentiellement un nombre important d'AC
  - Se rattacher à une AC mère implique de respecter a minima ses exigences minimales en matière de niveau de sécurité
- **Favoriser un découpage par population puis par usage** pour se rendre indépendant de l'organisation et éviter de multiplier le nombre d'AC (le RGS v2.0 renforce cette tendance)
- **Différencier gabarits & usages !**
  - Deux porteurs utilisent des certificats basés sur le même gabarit si :
    - Les usages sont identiques
    - Si les processus de gestion de ces certificats sont régis par les mêmes mesures de sécurité



Sécuriser l'autorité de certification

- Les AC qui n'émettent pas de certificats aux entités finales sont mis **hors ligne ou déconnectés**

Stockage des clés privées de l'AC

Sécuriser les clés privées des AC

La **compromission** de la clé privée de l'AC entraîne la compromission de tous les certificats émis par l'AC

- Stockage des clés privées des AC
  - **HSM (Hardware Security Module)** pour les AC opérationnelles
  - Certificat logiciel pour les AC hors ligne ou déconnectées
  - Uniquement si l'accès physique aux machines hors ligne est strictement restreint (Live CD dans coffre fort)

Type de HSM

- 2 types de HSM
  - **Carte HSM** : carte physique pour serveur
  - **Boîtier HSM** : périphérique réseau
    - Permet la mutualisation du HSM pour plusieurs serveurs d'AC

Avantages d'un HSM

- **Accélération matérielle** pour les opérations cryptologiques
  - Plus de risque de goulot d'étranglement
- Allège les **contraintes d'accès physique**
- Permet le partage des secrets avancés **(n parmi m)**
  - Plusieurs cartes à puces disposant d'un bout de la clé privée de l'AC sont remis à plusieurs personnes (directions métiers, RSSI, DSI, DG, etc.)
  - Séparation des pouvoirs
- Respecte les standards PKCS#11, OpenSSL, Microsoft CAPI, etc.
- Très robuste contre les attaques de sécurité

Même pour le niveau * de la RGS, il faut un HSM

Certificats

Renforcer la sécurité des certificats

/ Algorithme de « chiffrement »

- **RSA** : authentification, signature, chiffrement
- DSA : authentification, signature

/ Taille des clés

- **4096** bits pour les AC
- **2048** bits pour les entités finales
- 1024 dans certains cas pour des soucis de performance mais non recommandé par RGS

/ Algorithme de hachage

- **SHA-2** recommandé (SHA-256 ou 512) par RGS

Non supporté sur les postes clients Windows XP (SP2 ou inférieur) ; SHA-1 uniquement

/ Durée de vie

- AC racine et intermédiaire **20 ans**
- AC émettrice **10 ans**
- Porteur **3 ans**
  - Implique le renouvellement du certificat de l'AC émettrice tous les 7 ans au plus

Stocker le bi-clé sur un support sécurisé

/ Application / Serveur

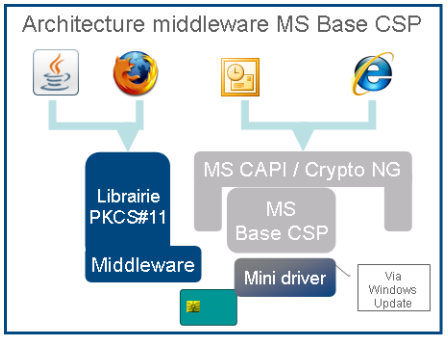
- Certificat logiciel dans la plupart des cas puisque l'exploitation est maîtrisée
- HSM pour les applications critiques

/ Porteur

- Choix du support
  - Authentification forte
- Carte à puce
  - Choix du middleware
  - BaseCSP dans l'entreprise
  - IAS dans l'administration

Minimiser l'impact sur les postes clients

Prévoir la compatibilité avec les applications non BaseCSP



Listes de révocation

La révocation est souvent présentée comme le talon d'Achille d'une PKI

/ Publication des listes de révocation

- Type de publication
  - L'AC racine publie la liste des autorités révoquées (LAR)
  - Les AC émettrices publient les listes de révocation de certificats (LCR)
  - Delta LCR
- Fréquence de publication
  - **24h** pour les LCR
- Lieu de publication
  - **LDAP** pour l'accès en interne
  - **HTTP** pour l'accès distant

/ Gabarit des certificats

- **CRLDP** à renseigner dans les certificats
  - Mettre l'URL de publication des LCR et LAR dans les certificats

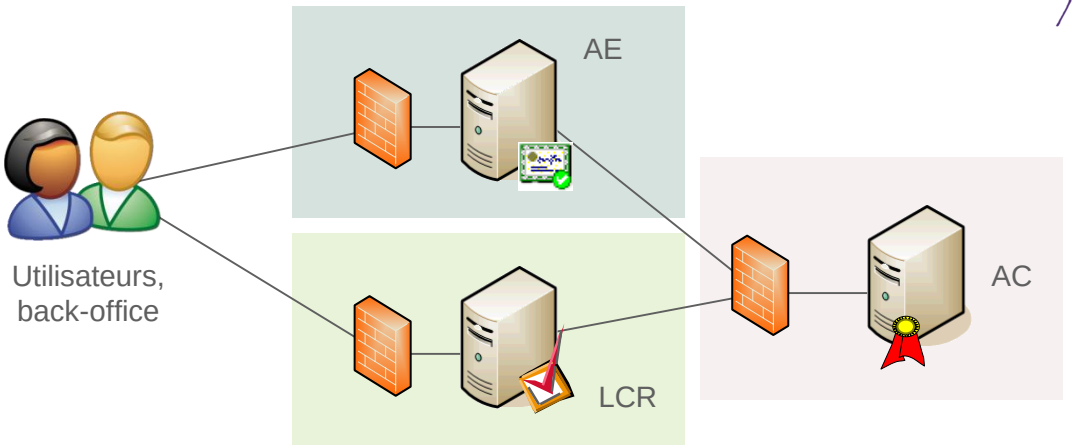
/ Problème d'expiration des LCR sur les postes clients

- Le protocole **OCSP** permet de vérifier un certificat en temps réel
  - Encore peu déployé

Architecture technique

Architecture technique recommandée

- Isolation des services PKI
  - **AC racine hors ligne**
  - **AC dans une DMZ sécurisée dédiée**
  - Firewall entre AC et AE
    - Dialogue entre l'AC et l'AE en SSLv3/TLS avec certificat
  - Serveurs à placer dans **des DMZ Internet** :
    - Serveur de publication des LCR et LAR en HTTP
    - Serveur AE si les opérations d'enregistrement peuvent se faire depuis un réseau distant



Contraintes techniques

- **Accès physique restreint** aux machines PKI
- Serveur dédié et indépendant pour
  - L'opérateur de certification
  - L'opérateur d'enregistrement (CMS)
- OS Sécurisé
  - Mises à jour de sécurité effectuées régulièrement
- Séparation des pouvoirs
  - Plusieurs profils pour les opérations d'administration
- Haute disponibilité des services
  - Ou a minima, prévoir du matériel de remplacement

Avec la PKI Microsoft, l'architecture idéale est difficilement réalisable (forte adhérence entre Active Directory et l'AC)

Organisation

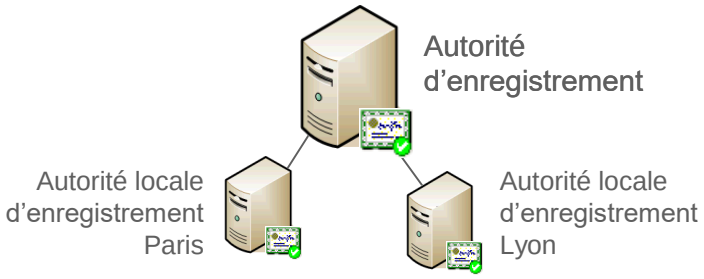
Mettre en place une équipe PKI dédiée

/ Équipe **exploitation**

- Rôles
  - Administration et maintenance
  - Support avancé
  - Supervision (surveillance de publication des LCR, contrôle de l'arrivée à expiration des certificats des AC)
- Qualification et compétences
  - Compétences techniques suffisantes
  - Connaissances du contexte de l'entreprise

/ Équipe **enregistrement**

- Équipe dédiée pour l'interface entre l'autorité d'enregistrement et les porteurs de certificat
- Découpage métier et géographique pour les autorités d'enregistrement



Réutiliser l'organisation existante pour définir les processus de gestion des certificats

/ **Séparation des rôles**

- Ne pas accumuler des rôles contradictoires (création et validation de certificats par exemple)

Avec la PKI Microsoft, séparation des rôles parfois difficile. Par exemple, admin PKI et admin Active Directory

/ **Intégration la plus transparente possible** dans les processus existants

- Quelques exemples…
  - A l'arrivée d'un collaborateur, le responsable hiérarchique demande la création d'un certificat en même temps que l'ordinateur portable ou le téléphone portable
  - Bureau des badges unique
- Contraintes fortes si le niveau de sécurité attendu est élevé
  - Par exemple, vérification de l'identité en face à face systématique
  - Gestion des modes dégradés

Prévoir les processus d'exploitation et démarches liées à la PKI

- Quelques **processus récurrents à prévoir**, conformément à la RGS
  - Audit de conformité de l'ensemble de la PKI
    - 1 fois par an pour RGS ***
    - 1 fois tous les 3 ans pour RGS *
  - Analyse complète des journaux d'événements
    - 1 fois par jour ouvré pour RGS ***
    - 1 fois toutes les 2 semaines pour RGS *

- Démarches uniques
  - Enregistrement auprès de la **CNIL** pour le stockage de données personnelles
  - Demande d'un **OID à l'AFNOR**

La PKI, un service d'infrastructure mûr et maîtrisé

Un service d'infrastructure incontournable

La PKI offre une réponse globale…

… à des besoins de sécurité hétérogènes

… à des besoins jusqu'alors mal adressés (notamment la signature électronique)

La PKI est une solution plébiscitée par le marché

Une forte volonté politique
- Reconnaissance légale de la signature électronique en Europe
- Un usage qui se généralise dans les administrations françaises (via les initiatives du SGMAP)

Une intégration progressive dans tous les produits

Une solution en cours d'adoption par les entreprises

La définition des orientations stratégiques : l'étape clé du projet

Adopter une démarche de mise en place progressive

Cibler d'abord les usages à fort enjeu
Pérenniser les investissements en concevant une infrastructure évolutive

Choisir une stratégie fournisseur adaptée

Internalisation : éditeur de logiciel
Externalisation : Opérateur de Certification

Choisir le support des certificats

Vers un **badge unique** au sein de l'entreprise ?

Préparer l'intégration de la PKI dans le SI

Avec les applications
Avec les référentiels utilisateurs (annuaires, *provisioning*)
Avec l'organisation existante

Des projets maîtrisés

Périmètre restreint
Construction : 6 mois, 400k€

Evolutivité

Périmètre global
Construction : 12 mois, 800k€ à 1M€

= 150 €/util./an

Hyp. : 1 000 utilisateurs

= 50 €/util./an

Hyp. : 50 000 utilisateurs

Construction (coûts amortis sur 5 ans)
Études, matériel, logiciels, intégration, pilotage

Exploitation
Gestion des certificats, *hot-line*, exploitation technique, maintenance

Cartes et clés à puce
Achat et renouvellements

WAVESTONE

Kévin GUÉRIN
Manager

M +33 (0)7 62 97 16 45
kevin.guerin@wavestone.com

wavestone-advisors.com
@wavestone_

PARIS

LONDON

NEW YORK

HONG KONG

SINGAPORE *

DUBAI *

BRUSSELS

LUXEMBOURG

GENEVA

CASABLANCA

LYON

MARSEILLE

NANTES

* Partenaires stratégiques