ÉCOLE SUPÉRIEURE D'ÉLECTRICITÉ

La vie privée sur Internet, une question de confiance ?

Guillaume Piolle
http://guillaume.piolle.fr/
guillaume.piolle@supelec.fr

Supélec - équipe CIDRE

Journée « Web et Confiance »
17 janvier 2013

La marchandisation des données personnelles

Influence de l'économie

Qu'on le regrette ou non, les données à caractères personnel sont devenus le « carburant » d'Internet, alimentant la publicité et le commerce électronique.

La marchandisation des données personnelles

Influence de l'économie

Qu'on le regrette ou non, les données à caractères personnel sont devenus le « carburant » d'Internet, alimentant la publicité et le commerce électronique.

Dans le même temps :

- Utilisateurs de plus en plus conscients des risques en matière de vie privée ;
- Utilisateurs de plus en plus exigeants dans le domaine ;
- Utilisateurs de plus en plus défiants vis-à-vis des différents acteurs du domaine.

La métaphore du « petit-cadenas-dans-le-coin-de-l'écran »

Le symbole de validation SSL/TLS
semble avoir acquis la confiance du public
pour la sécurité des communications.

Serait-il possible de construire
le même type de confiance
pour la protection de la vie privée sur Internet ?

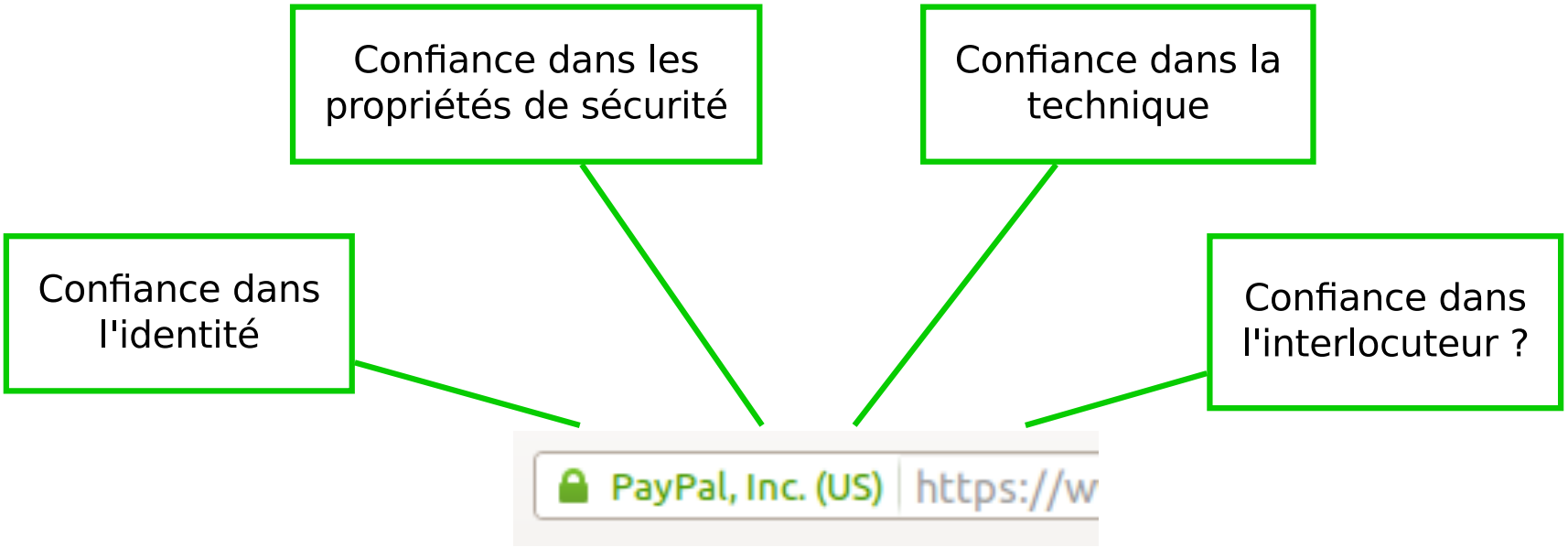
La métaphore du « petit-cadenas-dans-le-coin-de-l'écran »

Confiance dans l'identité

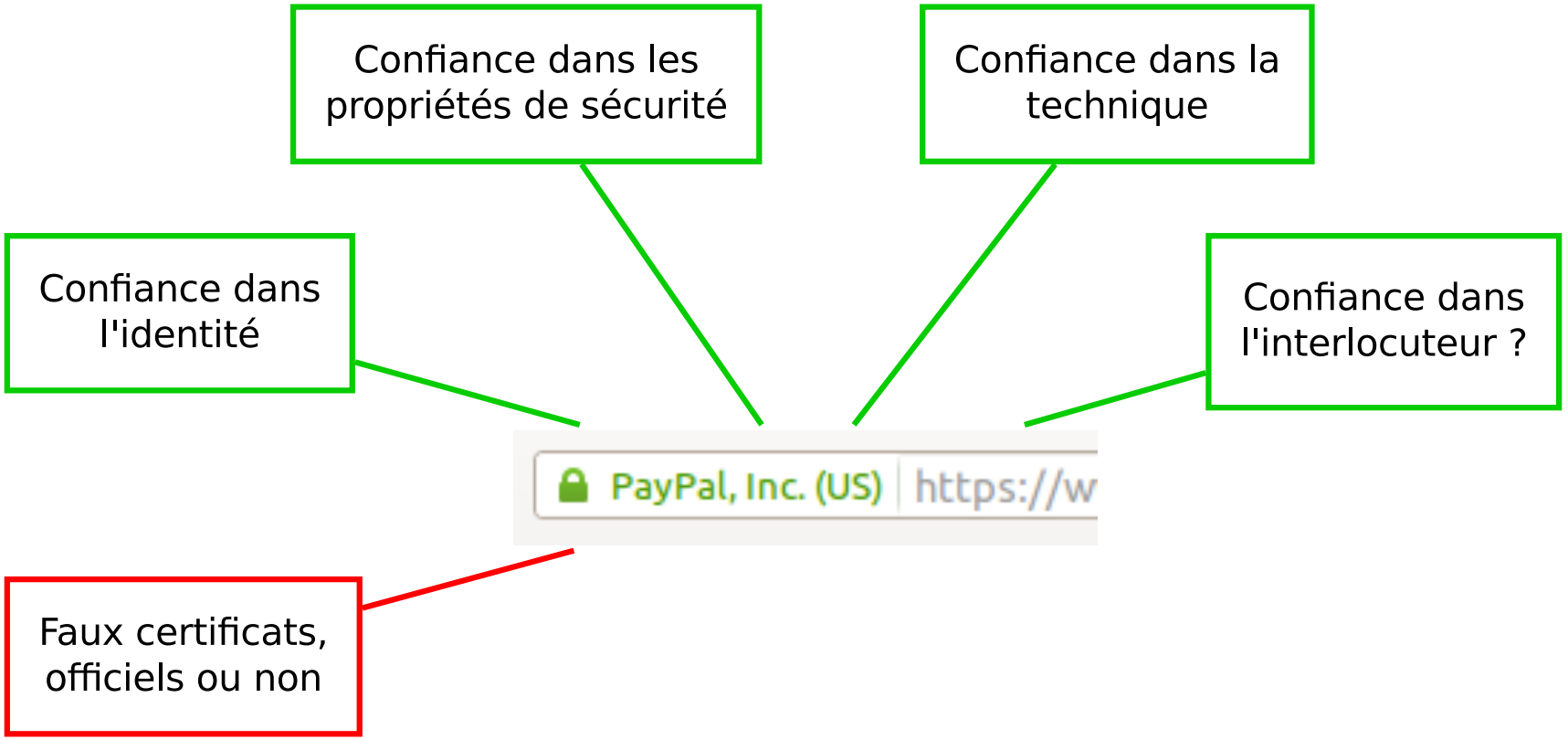
La métaphore du « petit-cadenas-dans-le-coin-de-l'écran »

La métaphore du « petit-cadenas-dans-le-coin-de-l'écran »

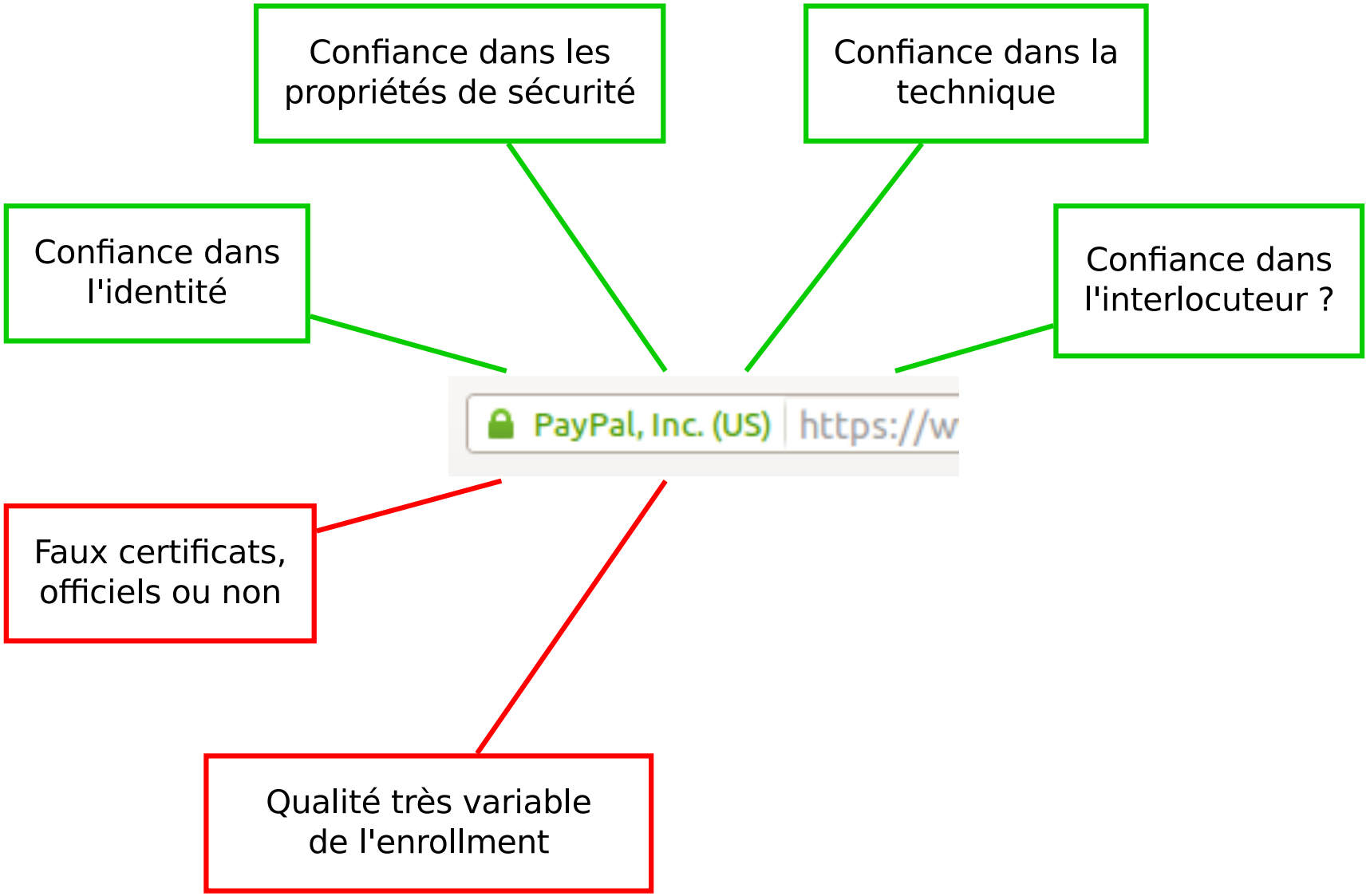
La métaphore du « petit-cadenas-dans-le-coin-de-l'écran »



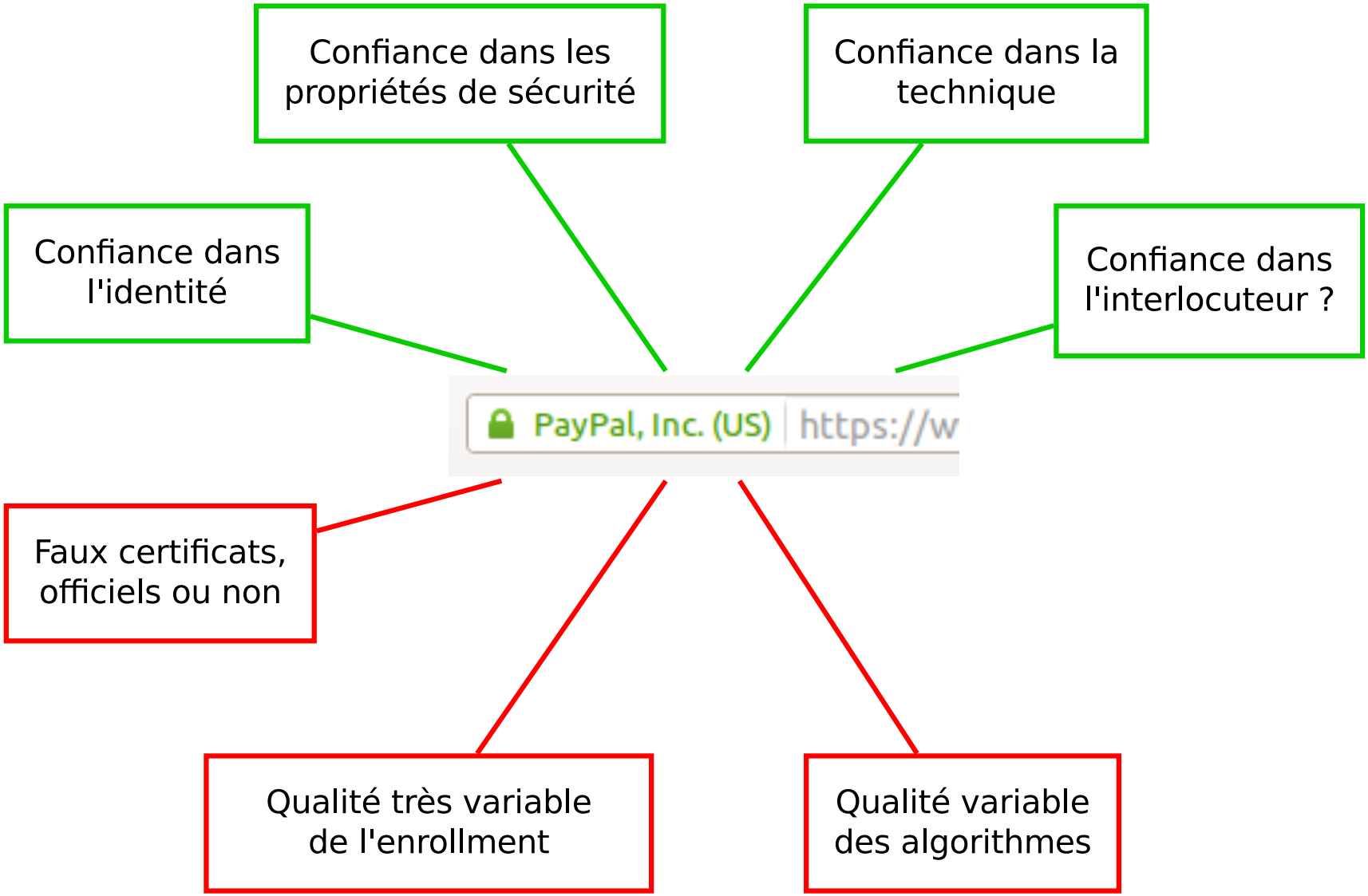
La métaphore du « petit-cadenas-dans-le-coin-de-l'écran »



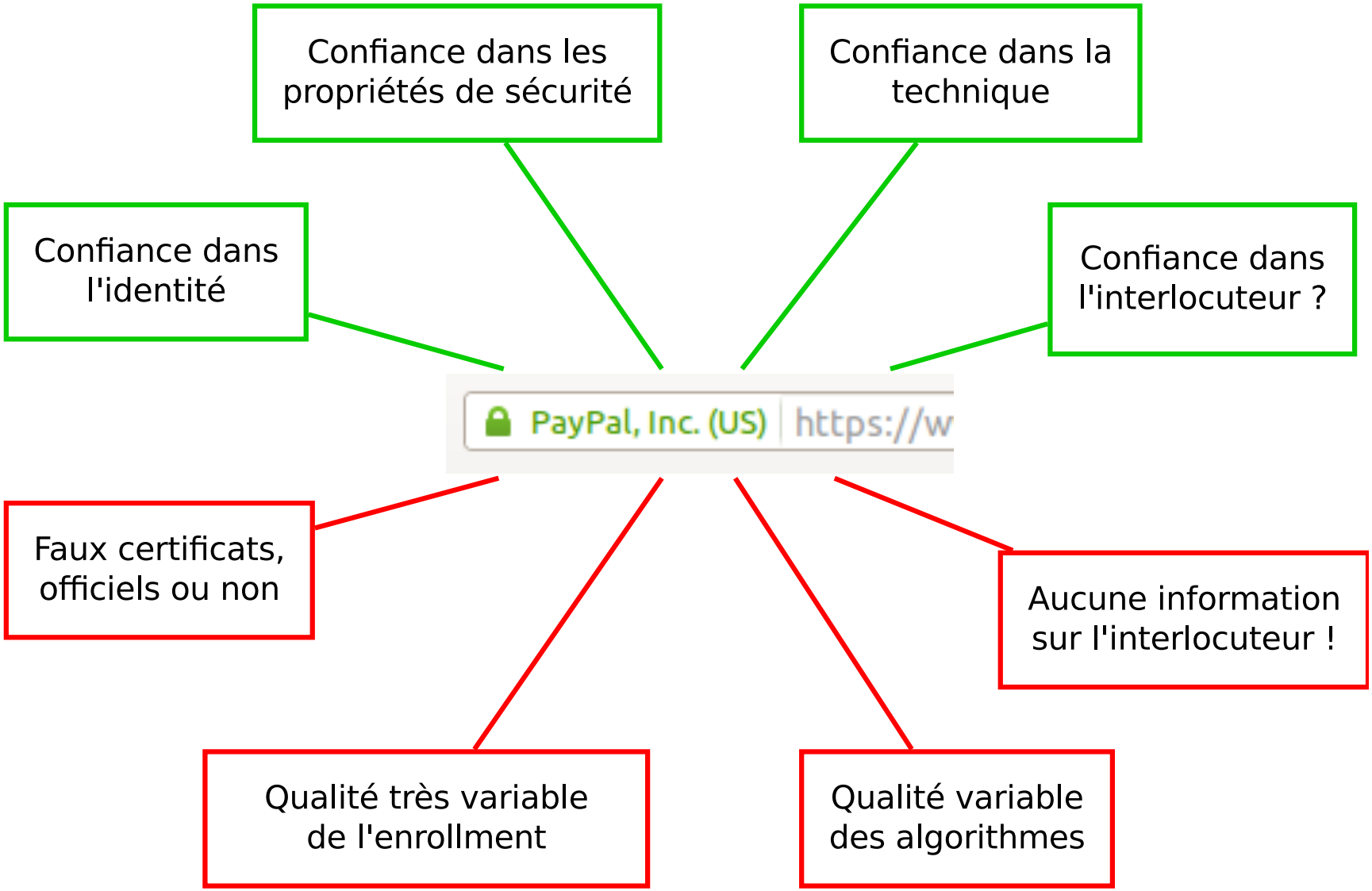
La métaphore du « petit-cadenas-dans-le-coin-de-l'écran »



La métaphore du « petit-cadenas-dans-le-coin-de-l'écran »



La métaphore du « petit-cadenas-dans-le-coin-de-l'écran »



La protection de la vie privée selon l'ISO

Common Criteria for Information Technology Security Evaluation

Norme ISO/IEC 15408, successeur de l'*Orange Book* du DoD.
Section 7 : protection de la vie privée.

Exigences techniques pour assurer la vie privée

- **Anonymat** (*anonymity*) : incapacité des observateurs à déterminer l'identité d'un utilisateur ;
- **Pseudonymat** (*pseudonymity*) : idem, mais en imposant à l'utilisateur de répondre de ses actions ;
- **Non-chaînabilité** (*unlinkability*) : incapacité des observateurs à déterminer si deux actions ont été réalisées par le même utilisateur ;
- **Non-observabilité** (*unobservability*) : incapacité des observateurs à déterminer si une action est en cours.

La protection des données personnelles

- Obligation d'information ;
- Importance du consentement ;
- Droits d'accès, d'opposition, de rectification, de suppression ;
- Principe de finalité ;
- Principe de proportionnalité ;
- Limites à la conservation ;
- Limites à la diffusion ;
- Obligation de sécurité.

Principes de **minimisation** et de **souveraineté**

L'observabilité des violations

Un schéma classique pour la confiance

- Partir d'une confiance « par défaut » en une entité ;
- Mettre à jour cette confiance en fonction d'un résultat observé (*outcome*, respect des normes. . .) ;
- Mettre à jour cette confiance en fonction des recommandations provenant d'autres agents.

L'observabilité des violations

Un schéma classique pour la confiance

- Partir d'une confiance « par défaut » en une entité ;
- Mettre à jour cette confiance en fonction d'un résultat observé (*outcome*, respect des normes. . .) ;
- Mettre à jour cette confiance en fonction des recommandations provenant d'autres agents.

Problème :

La majorité des violations en termes de protection des données personnelles sont difficilement observables !

L'observabilité des violations

Comment déterminer si. . .

- Une information a été indûment collectée ?
- Une information a été indûment partagée ?
- Une information a été indûment conservée ?
- Une information a été mise en corrélation avec une autre ?
- Une information a été utilisée dans un calcul ?

L'observabilité des violations

Comment déterminer si. . .

- Une information a été indûment collectée ?
- Une information a été indûment partagée ?
- Une information a été indûment conservée ?
- Une information a été mise en corrélation avec une autre ?
- Une information a été utilisée dans un calcul ?

Pistes

Obligations d'auditabilité (par qui ?), indiscrétions des prestataires, plates-formes « contraintes », utilisation de tiers de confiance, *remote execution*. . .

L'observabilité des violations

Comment déterminer si. . .

- Une information a été indûment collectée ?
- Une information a été indûment partagée ?
- Une information a été indûment conservée ?
- Une information a été mise en corrélation avec une autre ?
- Une information a été utilisée dans un calcul ?

Pistes

Obligations d'auditabilité (par qui ?), indiscrétions des prestataires, plates-formes « contraintes », utilisation de tiers de confiance, *remote execution*. . .

Risque additionnel de la désanonymisation de bases de données

La confiance dans les experts

Le difficile établissement de la confiance dans un procédé technique

- Le procédé n'est généralement pas compréhensible directement par le grand public, qui ne peut se faire une opinion éclairée ;
- Seul un expert peut valider la qualité du procédé ;
- L'expert ne bénéficie pas par nature de la confiance du public ;
- Les conditions de l'expertise (cible, hypothèses, environnement) peuvent jouer en défaveur de cette confiance ;
- Tout expert peut être pris en défaut.

La confiance dans les experts

Peut-on concevoir des procédés dont les propriétés puissent paraître évidents au grand public ?

La confiance dans les experts

Peut-on concevoir des procédés dont les propriétés puissent paraître évidents au grand public ?

Peut-on concevoir des procédés qui embarquent directement la preuve de leurs propriétés ?

La confiance dans les experts

Peut-on concevoir des procédés dont les propriétés puissent paraître évidents au grand public ?

Peut-on concevoir des procédés qui embarquent directement la preuve de leurs propriétés ?

Et la confiance dans la preuve ?

Le grand public risque de ne pas avoir davantage confiance dans une preuve, produit d'un système formel qu'il ne comprend pas, auquel il n'adhère pas, auquel il ne « croit » pas.

La confiance dans le contexte juridique

Les Français ont une relation presque affective à la loi « Informatique et Libertés ».

Mais. . .

- Quelle adaptation des textes aux risques techniques en termes de vie privée ?
- Quelle confiance dans l'application et l'effectivité des textes ?
- Quelle confiance dans les procédures instaurées (saisine de la CNIL, saisine du procureur, médiation, sanctions, CIL. . .) ?
- Quelle confiance dans la CNIL ?

Le risque de la labellisation

Le cadre juridique autorise la CNIL à délivrer des « labels » relatifs à la protection des données personnelles.

- Pour l'instant : formations, procédures d'audit ;
- Dans le futur : plates-formes, traitements, applications ?

Le risque de la labellisation

Le cadre juridique autorise la CNIL à délivrer des « labels » relatifs à la protection des données personnelles.

- Pour l'instant : formations, procédures d'audit ;
- Dans le futur : plates-formes, traitements, applications ?

Risque d'une confiance indûe

La confiance dans « labels » de vie privée devrait dépendre :

- Des exigences d'audit (fréquence, publicité. . .) ;
- De la confiance dans les auditeurs ;
- D'une bonne connaissance de la cible de labellisation ;
- D'une bonne connaissance des propriétés auditées ;
- Des garanties sur la stabilité du système entre les audits.

Vie privée et transactions électroniques

Besoins en données essentiels à la transaction

- Argent ou preuve de paiement ;
- Biens échangés (ou informations de livraison) ;
- Éventuellement, non-répudiation.

Vie privée et transactions électroniques

Besoins en données essentiels à la transaction

- Argent ou preuve de paiement ;
- Biens échangés (ou informations de livraison) ;
- Éventuellement, non-répudiation.

Mais !

- Les sites marchands ont un intérêt à collecter des données d'usage liées à l'identité du client (profilage) ;
- Les sites marchands ont également un problème de **confiance**. Ils doivent s'assurer de l'identité réelle (et pas seulement des informations bancaires) de la personne qui transige.

Vie privée et transactions électroniques

Problématiques

Comment mettre en place une transaction marchande telle que :

- Le client ait confiance dans le fait que le site marchand ne puisse pas faire un lien entre lui et la transaction ?
- Le site marchand ait confiance dans le fait que la transaction se soit déroulée normalement ?
- Le site marchand ait confiance dans la possibilité d'identifier l'acheteur en cas de litige ?

Fournisseurs d'identités numérique

La version « pour de rire » : Idénum

- Le gouvernement, via l'ANSSI, labellise des fournisseurs ;
- L'utilisateur ouvre un compte auprès d'un fournisseur, à l'aide de sa carte d'identité (biométrique) ;
- On lui fournit un certificat attaché à un support physique ;
- Pour effectuer une transaction, il doit décliner son identité réelle et fournir le certificat garantissant son authenticité.

Fournisseurs d'identités numérique

Améliorations possibles (*si, si !*)

- L'utilisateur peut choisir son niveau d'enregistrement avec le fournisseur ;
- Le fournisseur permet à l'utilisateur de générer des certificats sur l'identité réelle ou sur des pseudonymes arbitraires ;
- L'utilisateur peut choisir d'utiliser un certificat (potentiellement pseudonyme) fournissant à ses interlocuteurs un niveau de confiance au choix, inférieur au niveau d'enregistrement.

Confiance et gestion de l'identité : Accréditations anonymes

Propriétés à assurer par un système d'accréditations anonymes :

1. Non-chaînabilité entre génération et utilisation d'une accréditation ;
2. Non-chaînabilité entre utilisations multiples d'une accréditation ;
3. Révélation partielle des attributs certifiés.

Confiance et gestion de l'identité : Accréditations anonymes

U-prove

Développé par la société Credentica, rachetée par Microsoft, spécifications publiques depuis 2010 (pour favoriser le support par les sites tiers).

- L'autorité de certification ne connaît pas l'identité du bénéficiaire et ne peut faire le lien avec l'utilisation des accréditations (prop. 1) ;
- La non-chaînabilité entre utilisations multiples (prop. 2) n'est pas assurée ;
- La révélation partielle (prop. 3) fonctionne de manière basique.

Idemix

Développé par IBM (principalement), dans le cadre du projet européen PrimeLife.

- Le contenu des certificats (pseudonyme) n'est pas transmis lors de la transaction (preuves *zero-K*), assurant la non-chaînabilité totale (prop. 1 et 2) ;
- La révélation partielle (prop. 3) fonctionne de manière plus riche.

Conclusion : niveaux de confiance

Problème général en protection de la vie privée

Comment garantir à l'utilisateur que les données qu'il transmet vont être traitées conformément à une politique de sécurité donnée, par un acteur dont il ne sait (presque) rien et sur lequel il n'a aucun contrôle ?

Contrôle de flux et contrôle d'usage distants

Conclusion : niveaux de confiance

Problème général en protection de la vie privée

Comment garantir à l'utilisateur que les données qu'il transmet vont être traitées conformément à une politique de sécurité donnée, par un acteur dont il ne sait (presque) rien et sur lequel il n'a aucun contrôle ?

Contrôle de flux et contrôle d'usage distants

Seule solution actuellement efficace

S'appuyer sur un contrôle du logiciel distant par du matériel certifié, pour empêcher l'exécution de programmes non prévus (*Trusted Computing*, mécanismes d'attestation).

Problèmes : mise en place et maintenance lourdes et coûteuses, confiance dans la certification sujette à caution, technologie présentant des risques pour la vie privée, l'autonomie et la libre concurrence.

Conclusion : points durs

De nombreux points durs en protection de la vie privée sont des problèmes de confiance :

- Comment établir une confiance de l'utilisateur dans une entité, dans un système, un protocole, une technologie ?
- Comment garantir que cette confiance reste fondée ?
- Comment mettre en place des transactions multi-parties dans lesquelles l'établissement de la confiance reste compatible avec la minimisation des données ?
- Comment se passer au maximum de tiers de confiance ?