Solutions de paiement embarquées

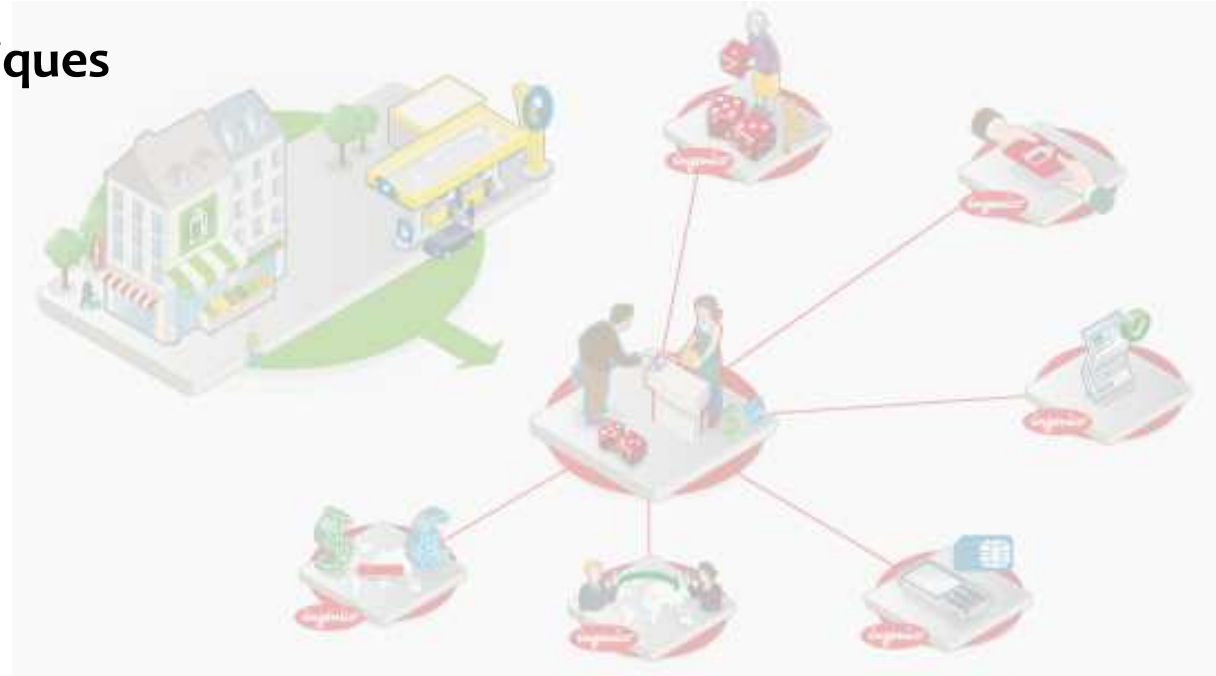
21 Octobre 2011

Matthieu Bontrond
Expert Cryptographie

ingenico®
beyond payment

Agenda

1. **Introduction à la monétique**
2. **Présentation de la société**
3. **Normes et Standards**
4. **Enjeux techniques**
5. **Perspectives**



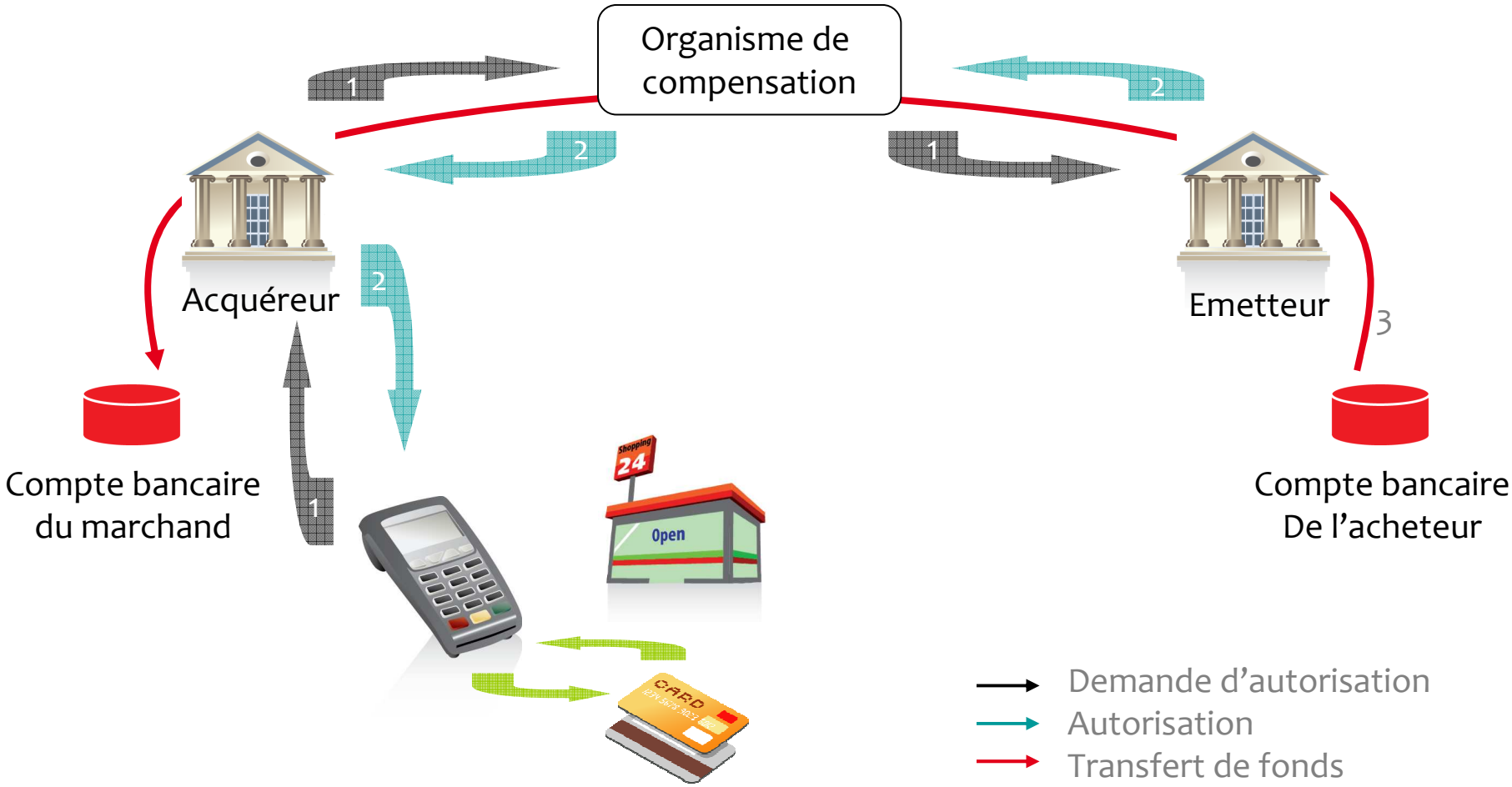
1 Introduction

Contraintes et Enjeux

ingenico®

beyond payment

La Monétique en bref



Contraintes et Enjeux

- **Des acteurs divers :**
  - Porteur (client)
  - Émetteur (banque du client)
  - Accepteur (commerçant)
  - Acquéreur (banque du commerçant)
- **Flux internationaux**
- **Nomadisme**
- **Variété des facteurs de forme :**
  - Cartes à puce
  - Bande magnétique
  - Sans contact (Carte/Mobile)
- **Réseaux de paiement différents :**
  - Visa
  - Mastercard
  - American Express
- **Des sujets connexes à la monétique:**
  - La billettique
  - La carte téléphonique
  - Le prépaiement
  - La carte cadeau dématérialisée (ou e-gift)
  - Le DCC (Dynamic Currency Conversion)
  - Le PME (Porte-monnaie Electronique)
  - Le paiement par téléphone mobile
  - Le marketing monétique
  - Le paiement sans contact (NFC)

2

Ingenico

Leader des solutions de paiement

beyond payment

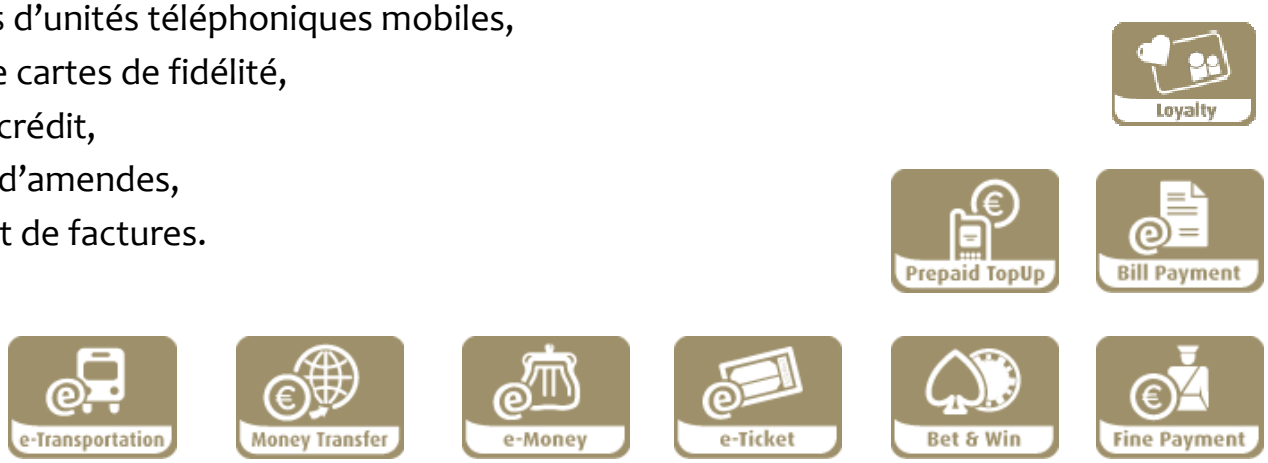
Produits et Activités de la Société

Produits :

1. **Terminaux de paiement et gestion de parc de terminaux**

Services :

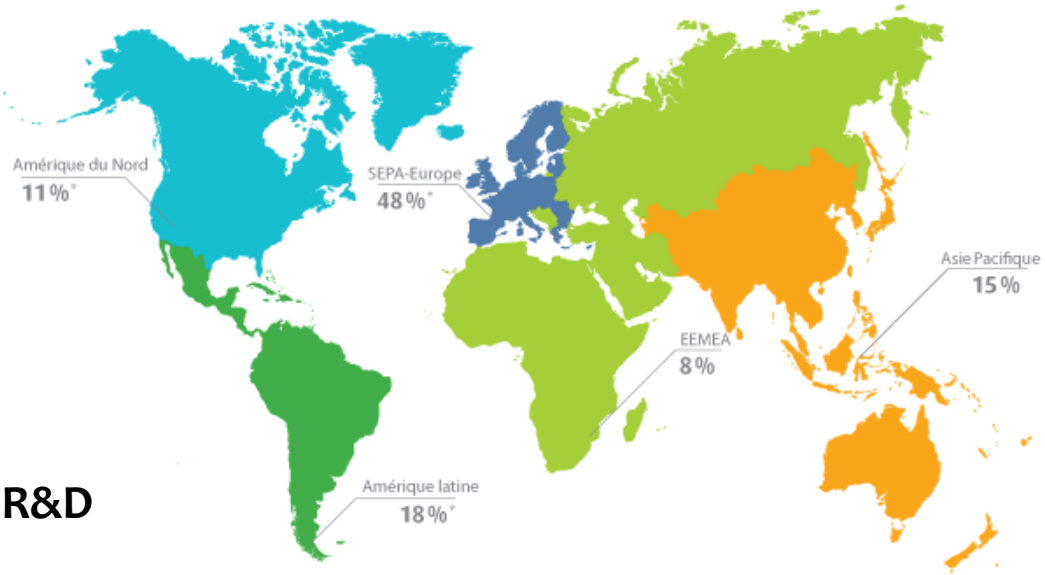
2. **Applications de paiement (locales, internationales, débit, crédit)**
3. **Services et solutions**
   - Transferts de crédit,
   - Recharges d'unités téléphoniques mobiles,
   - Gestion de cartes de fidélité,
   - Cartes de crédit,
   - Paiement d'amendes,
   - Règlement de factures.



Ingenico en chiffres

Leader sur le marché des terminaux de paiement

- 15 millions de terminaux en activité dans plus de 125 pays
- Plus de 3000 salariés répartis dans 40 pays
- 50 nationalités différentes représentées
- Chiffre d'affaires 2010 : 907 M€
- Plus de 30 ans d'existence
- 38% du marché mondial



Innovations

- Support de Google
- Support de Apple (ISMP)
- 8% des revenus investis en R&D

Une gamme de produits diversifiée

Mobile

Iphone®/Ipod touch®

Sans contact

Services

Biométrique

PDA

Signature

Santé

3 Mise en conformité

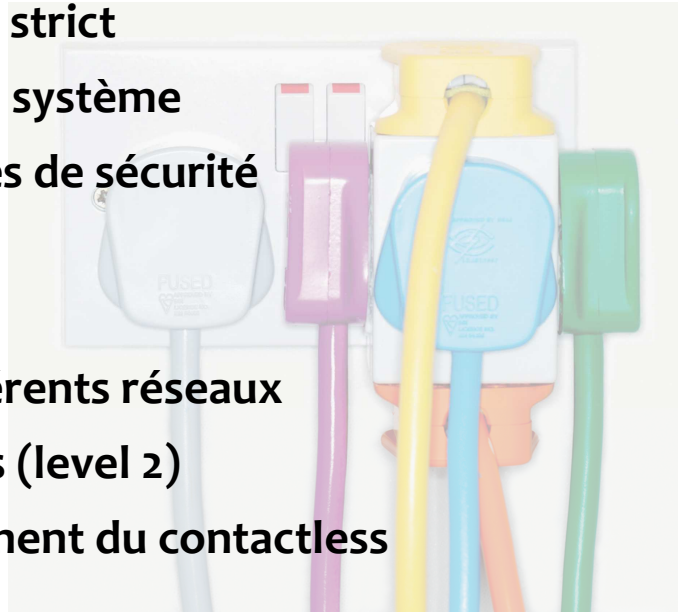
Normes et Standards

ingenico®
beyond payment

Normes internationales

Payment Card Industry

1. Garantir la sécurité des infrastructures de communication
2. Protéger les données du porteur de carte
3. Maintenir un système et des applications à jour
4. Mettre en œuvre un contrôle d'accès strict
5. Auditer régulièrement l'ensemble du système
6. Maintenir un ensemble de procédures de sécurité



EMV

> Permettre l'interopérabilité des différents réseaux
> Aspects matériels (level 1) et logiciels (level 2)
> Forte implication dans le développement du contactless

Normes nationales de Sécurité

Imposées par des groupements d'intérêt économique

> **ZKA (de), Interac (ca), APACS (uk), ABECS (br), APCA (au), PNC (Scandinavie)**
  - Certains pays se limitent au fonctionnel (par ex. GIE CB en France)

Single Euro Payements Area

> **Solution de paiement commune à 32 pays**
> **Interface commune à tous les utilisateurs**
> **Protocoles ouverts interopérables et standardisés**
> **Base législative commune**
> **Accès aux systèmes existants**
> **Réduction du nombre de certification**
> **Réduction des coûts de développement**

4

Enjeux techniques

Performances vs Sécurité

ingenico®
beyond payment

Performance exigée

Rapidité des transactions

> **Temps de transaction inférieur à 100 ms pour le contactless**

Fiabilité du matériel et disponibilité des équipements

> **Le paiement est la clef de toutes les activités des marchands**

> **Appareils dimensionnés pour des centaines de milliers de transactions**

- Lecteur de carte à puce
- Clavier d'entrée du PIN

Interopérabilité et Maintenance

> **Premiers systèmes mis en opération dans les années 80**

> **Contraintes liées à la compatibilité avec les systèmes existants anciens**

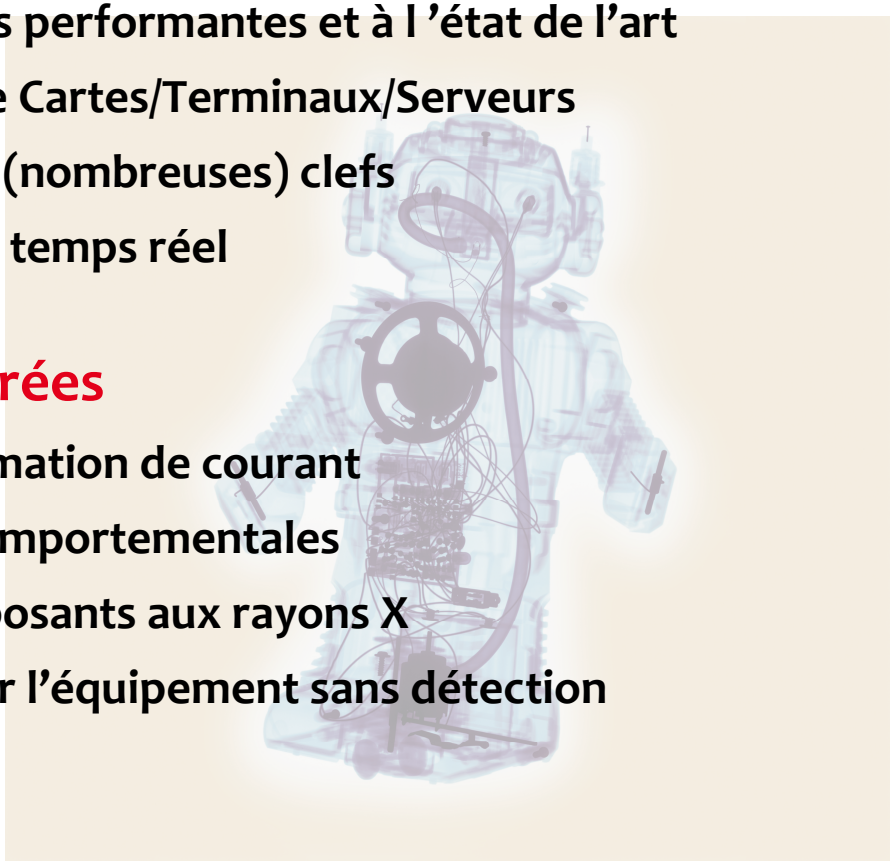
Sécurité attendue

Protocoles de communication robustes

- Primitives cryptographiques performantes et à l ’état de l’art
- Authentification dynamique Cartes/Terminaux/Serveurs
- Mécanismes de gestion des (nombreuses) clefs
- Vérification des données en temps réel

Attaques physiques contrées

- Pas d’analyse de la consommation de courant
- Résistant aux altérations comportementales
- Pas d’observation des composants aux rayons X
- Impossibilité d’ouvrir/percer l’équipement sans détection



5 Perspectives

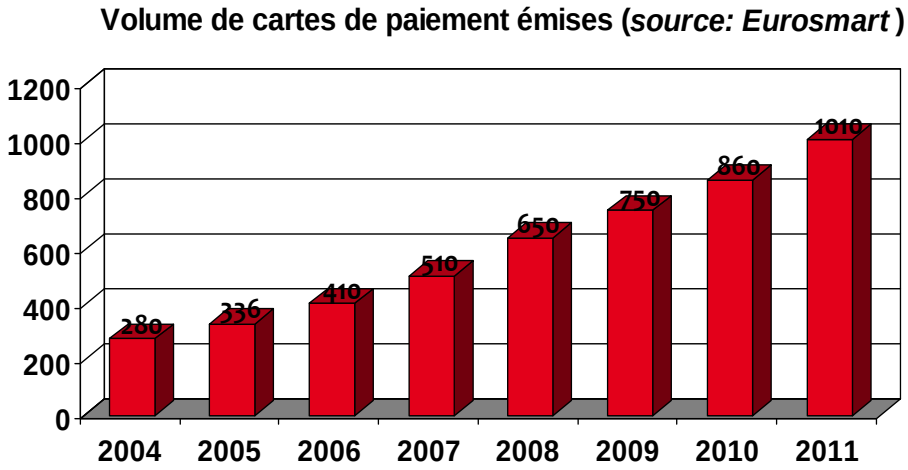
Défis pour demain

ingenico®

beyond payment

Evolution des habitudes de paiement

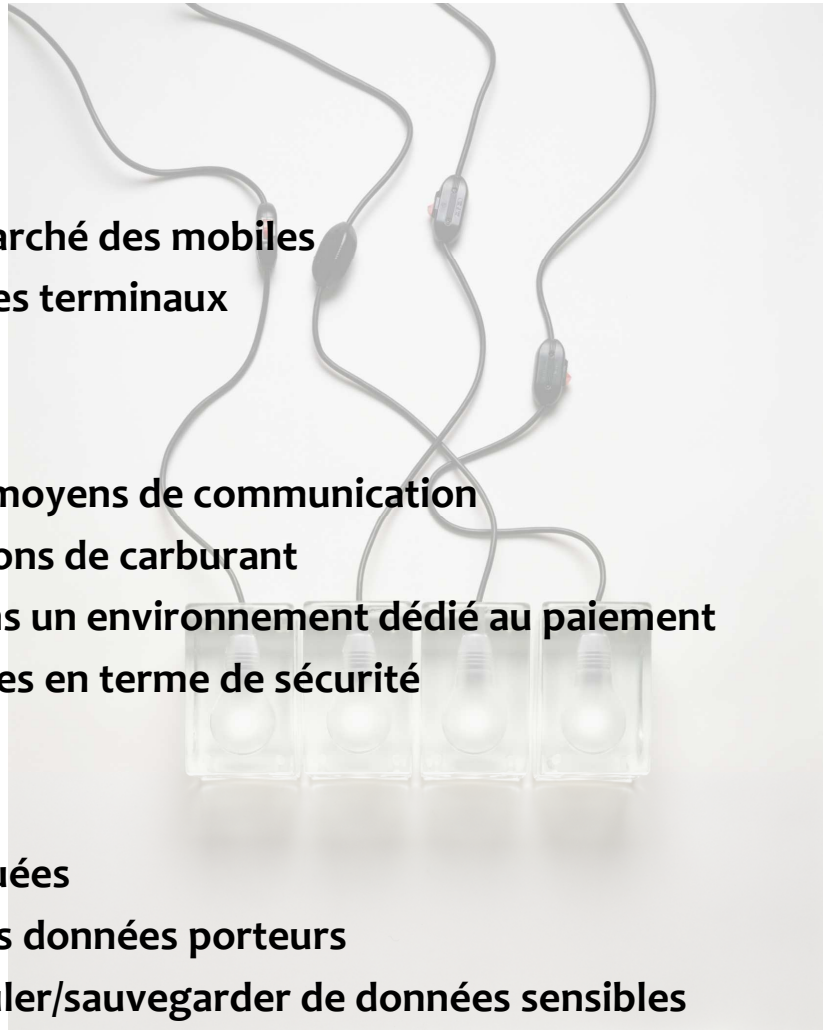
Un nombre croissant de transactions électroniques



Des utilisateurs toujours plus nomades

1. **Le paiement par mobile (la carte du porteur est dans son téléphone)**
2. **L'acceptation sur mobile (le commerçant initie et/ou accepte des transactions)**

Evolutions futures du marché



Design

- Exigences accrues des clients
- Demandes d'alignement avec le marché des mobiles
- Apparition des écrans tactiles sur les terminaux

Multimédia

- Évolution des technologies et des moyens de communication
- Diffusion de publicités sur les stations de carburant
- Ajout de contenus dynamiques dans un environnement dédié au paiement
- Ce dernier point pose des problèmes en terme de sécurité

Sécurité

- Attaques de plus en plus sophistiquées
- Développement du chiffrement des données porteurs
- Le commerçant ne doit pas manipuler/sauvegarder de données sensibles

Merci de votre attention
Avez-vous des questions ?

www.ingenico.com

ingenico®
beyond payment