

HOW TO ENHANCE BIOMETRIC APPLICATIONS TO PROTECT PRIVACY?

Vincent BOUATOU

Deputy Director, Strategic Innovation, IDEMIA



eu-LISA Industry Roundtable
**Biometric Technologies in Identity
Management and Verification**

WHY ARE BIOMETRIC APPLICATIONS SENSITIVE ?



Critical Missions

- Border Control
- Public Security
- Critical Facilities Access & Operation
- Criminal Investigations
- Digital ID
- ...



Sensitive Personal Data

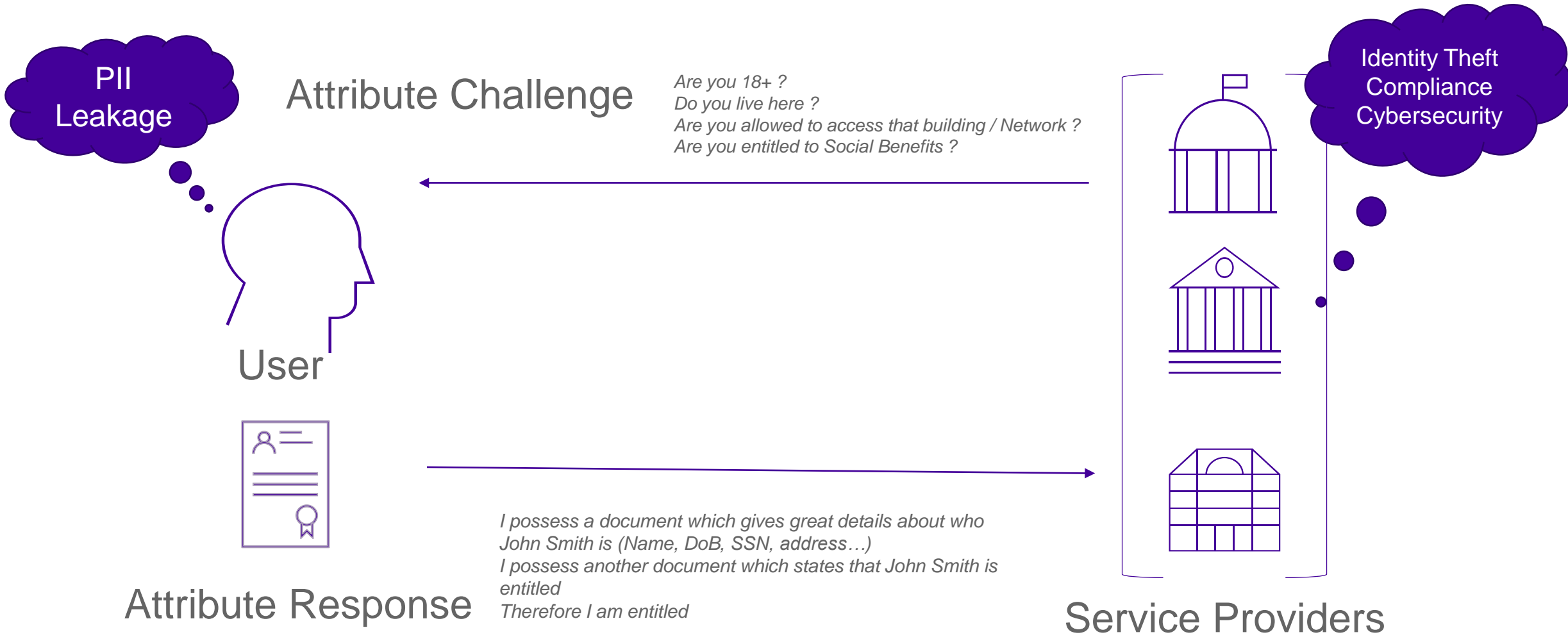
- Personal Identifying Information
- Non revocable Data
- Body-related images



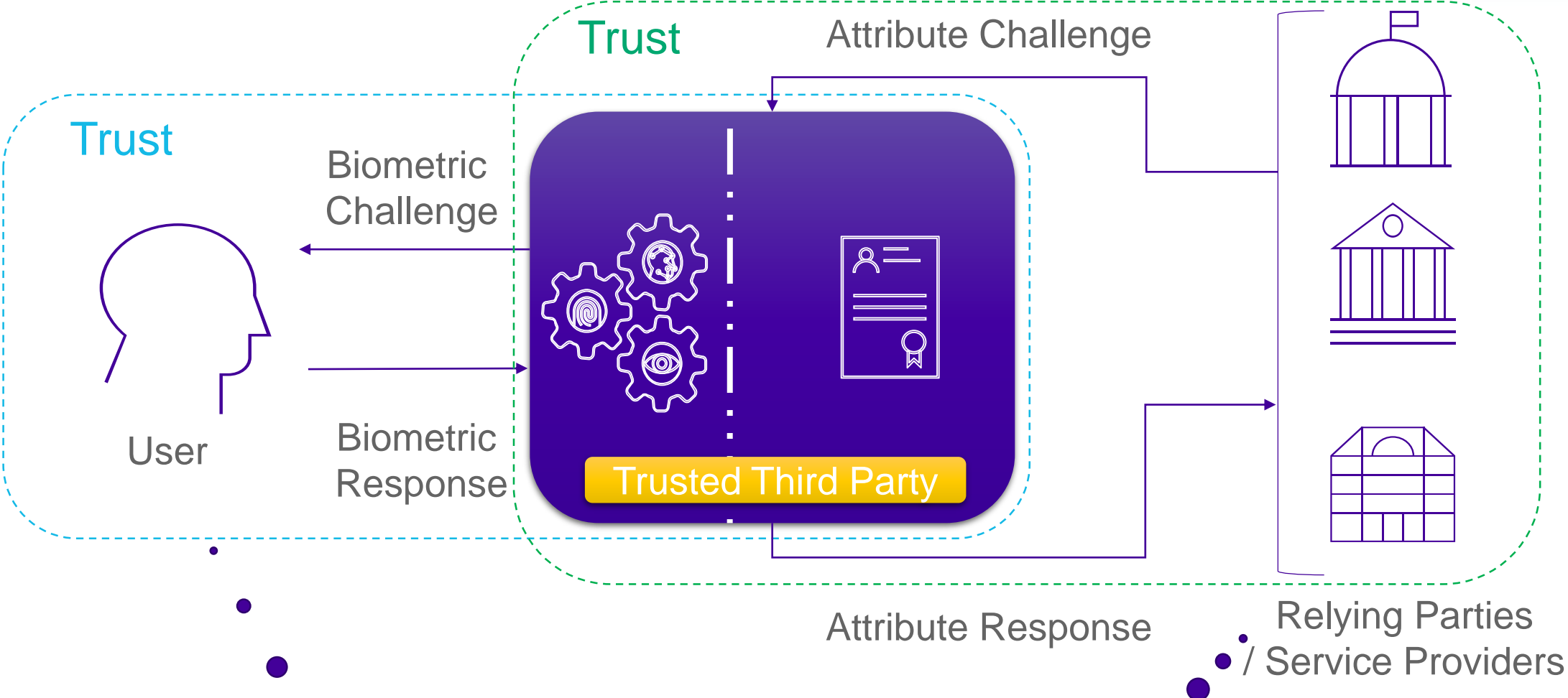
Mission Creep

- Organization
- Processes
- Compliance
- Protection by Design

TYPICAL INTERACTION BETWEEN SERVICE PROVIDER AND USER



MINIMAL DISCLOSURE SYSTEMS AS ENABLED BY BIOMETRICS





Minimal Disclosure
of PII



Biometric Verification
ensures formal Identification

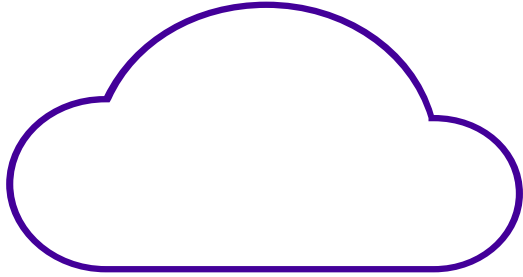
DIFFERENT APPROACHES



	Architecture	User Trust	Service Provider Trust	Strengths	Weaknesses
	Centralized Database			User Convenience Cost	Privacy
	Smart Card (Gov. issued)			Security Privacy	User Convenience Cost
	Personal Device (e.g., Smartphone)	 / 		User Convenience Ubiquity Privacy	Security

PRIVATE & SECURE COMPUTING

Driven mainly by Cloud Operations adoption



› **There is no cloud... It's just another person's computer**

› **Developments driven by development of cloud technologies and sovereignty issues**

- Can anyone access my data ?
- Can anyone tamper with the computations, which are performed in the cloud ?

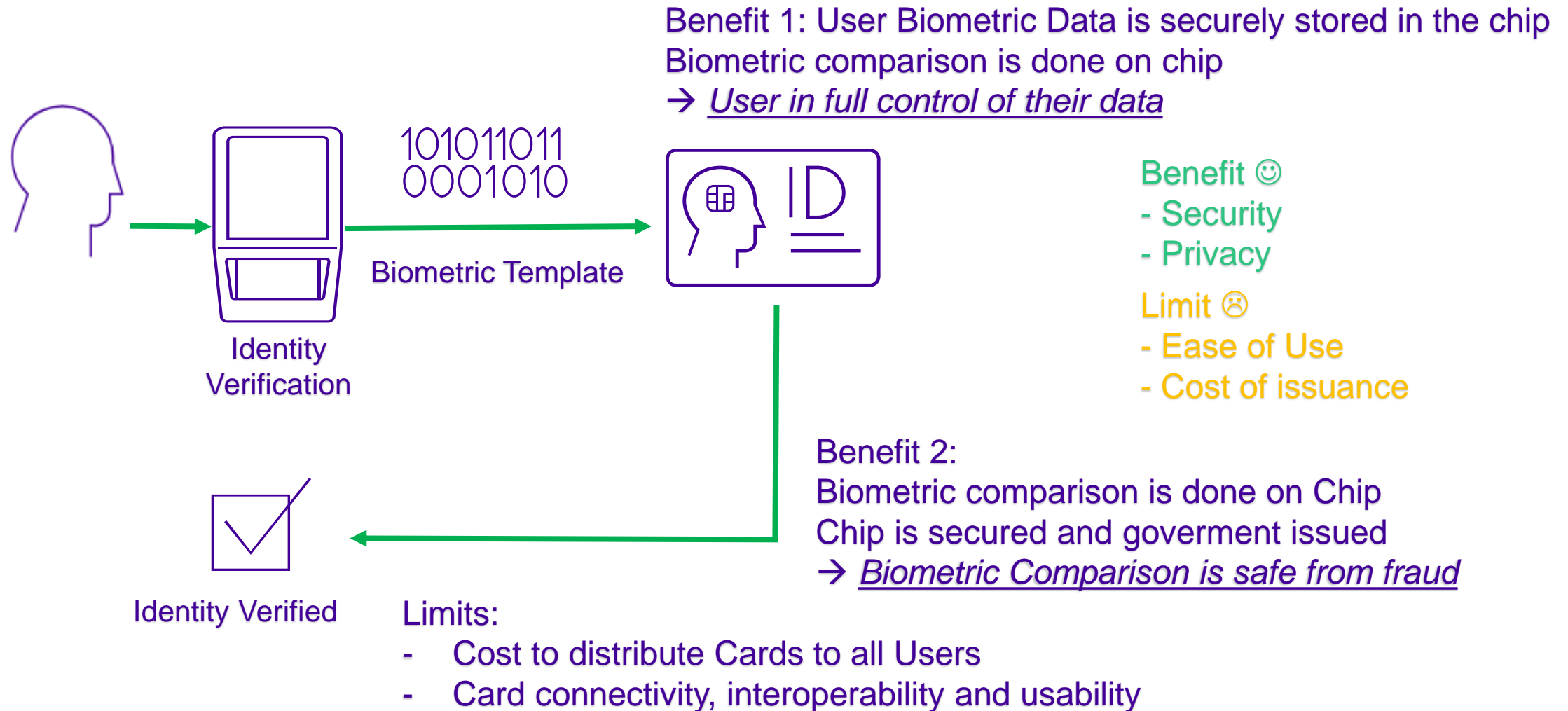
› **Significant interest to develop safeguards and protection for cloud operations**

- By Cloud Services Users
- By Cloud Service Providers

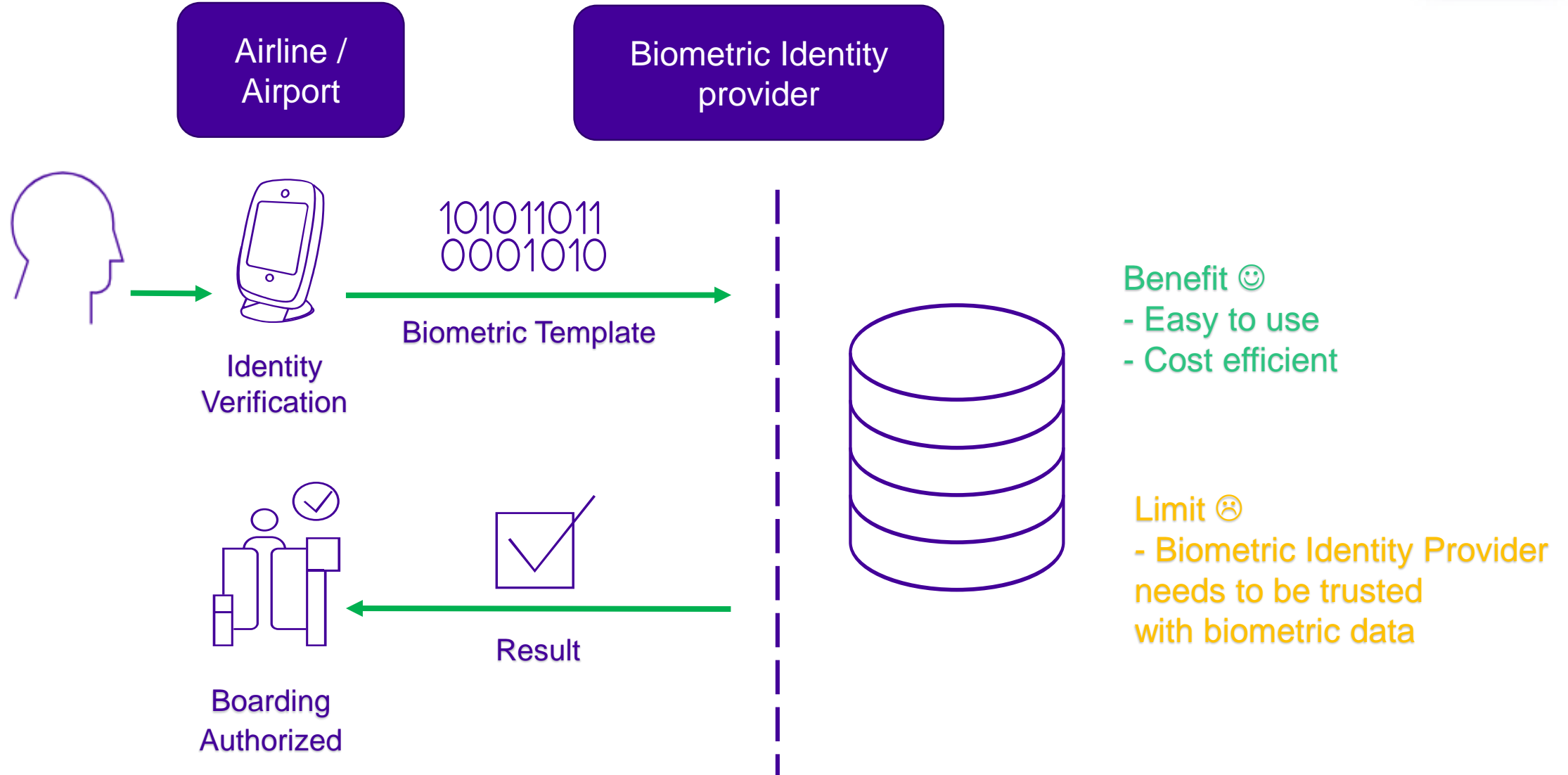
› **Technologies / approaches:**

- Full Homomorphic Encryption:
 - perform computation directly on encrypted data, with no access to result
- Secure Multipartite Computation:
 - no single entity can access the data or the computation
- Verifiable Computing:
 - trusting a computation, without having to trust the entity in charge of the computation, and with no access to data

USE CASE #1 : IDENTITY VERIFICATION USING SMART ID CARD

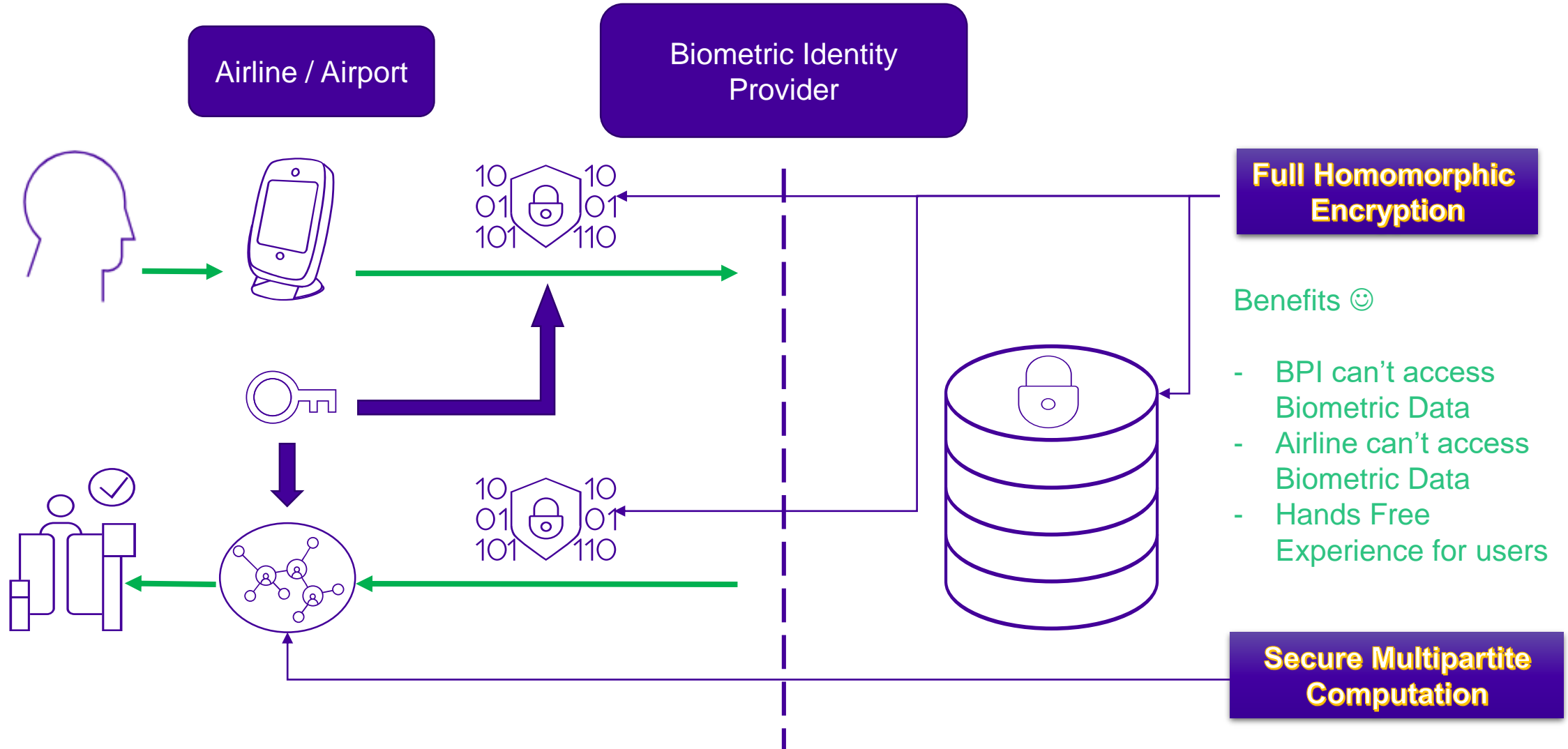


USE CASE #2 : AUTOMATED BOARDING WITH CENTRALIZED DATABASE

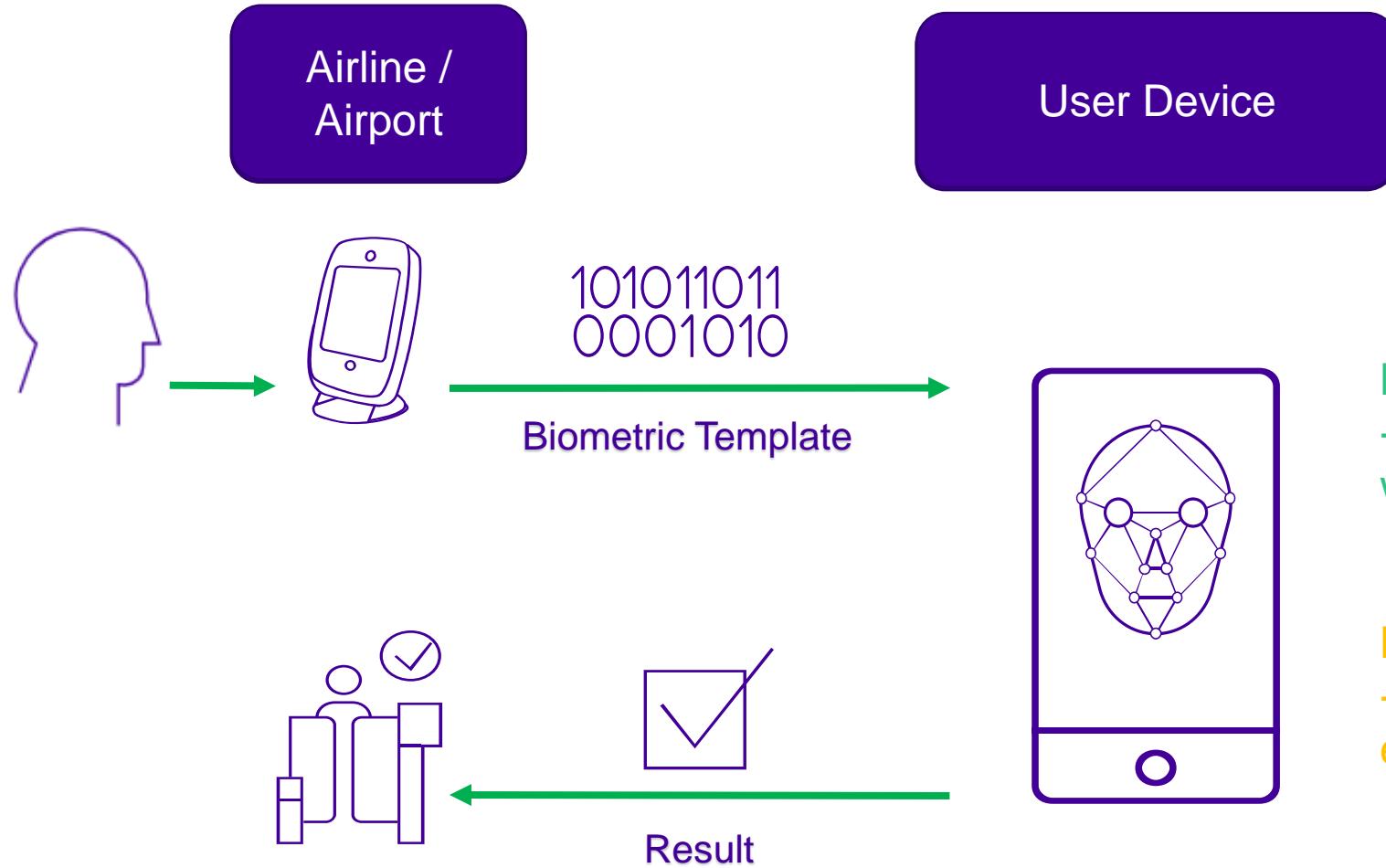


USE CASE #2: HOW TO ENHANCE PRIVACY

Full Homomorphic Encryption (FHE) + Secure Multipartite Computation (SMC)



USE CASE #3 : AUTOMATED BOARDING WITH PERSONAL DEVICES



Benefit 😊

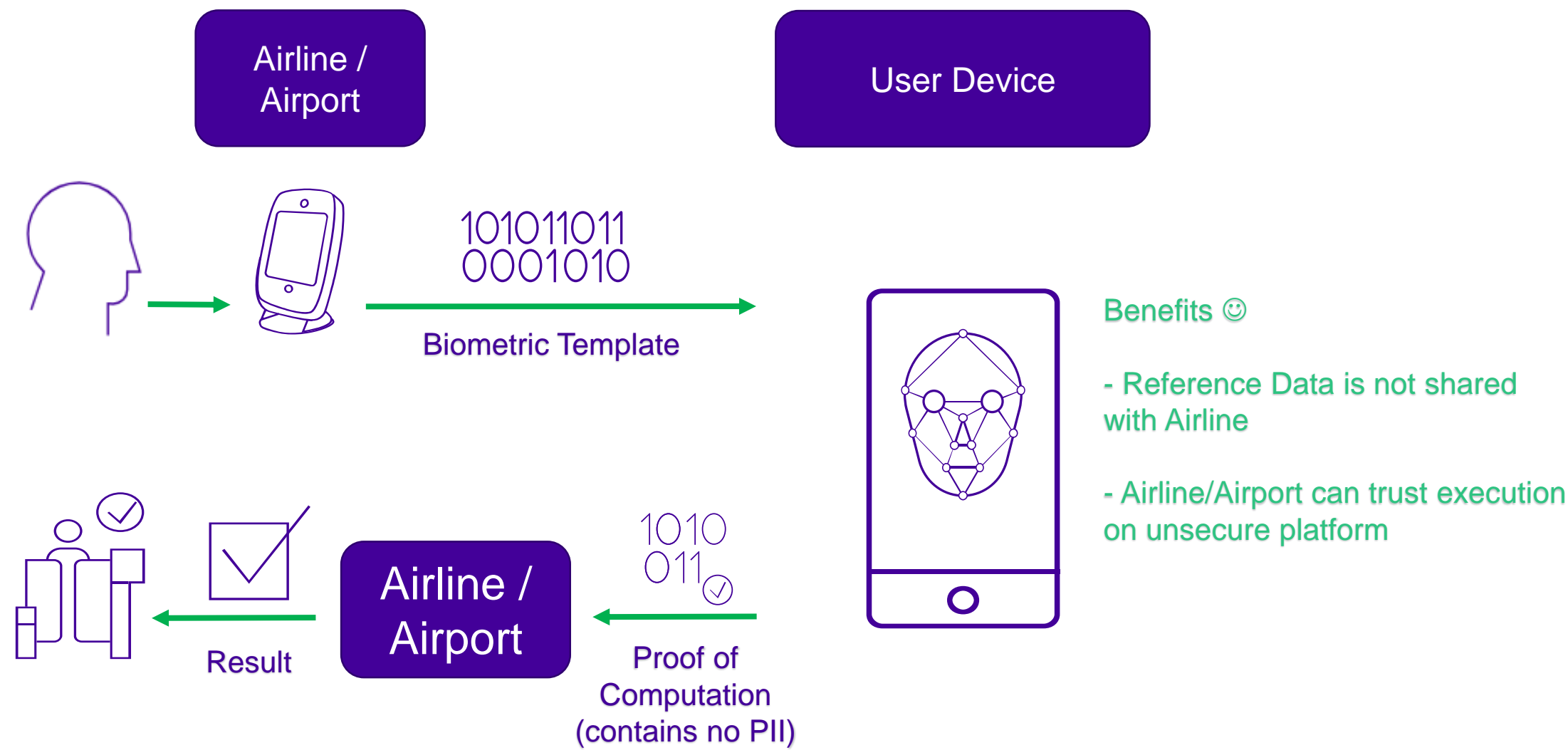
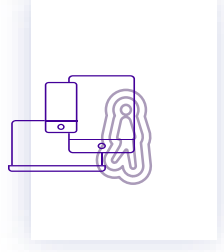
- Reference Data is not shared with Airline

Limit 😞

- Airline/Airport must Trust execution on unsecure platform

USE CASE 3: HOW TO ENHANCE SECURITY

Verifiable Computing



IN A NUTSHELL



	Architecture	Techniques	User Trust	Service Provider Trust	Strengths	Weaknesses
	Centralized Database	FHE + SMC			User Convenience Cost	Privacy
	Smart Card (Gov. issued)	N/A			Security Privacy	User Convenience Cost
	Personal Device (e.g., Smartphone)	Verifiable Computing			User Convenience Ubiquity Privacy	Security

Technology solutions exist to alleviate issues once they are formulated:

- Full Homomorphic Encryption + Secure Multipartite Computation provide the possibility to host PII on a central storage without risk of leak or misuse ;
- Verifiable Computing provides the possibility to trust a calculation which was performed by an unsecure, untrusted platform

KEY TAKE AWAYS



- › **Protecting Personally Identifiable Information (PII) and privacy requires an approach tailored to use cases because:**
 - Mission Creep risks are different
 - Risks on personal data are different
- › **Many techniques and technologies are being developed and when combined, they will be able to solve many issues considered to be a “risky processing” operation**
 - The two examples mentioned in this presentation are only examples, many other techniques exist
- › **It only takes a careful examination of each use case to propose the right solution**
 - The risk-based approach of the European Commission for the AI Regulation project also follows this line of reasoning
 - In a world where technological development is accelerating, describing the essential requirements in functional and technical terms is better than mandating how technologies must be developed and deployed, as nobody knows what technologies and capabilities may appear in the future
- › **Large and transverse technology bans can stifle innovation**



Vincent BOUATOU
Strategic Innovation
Public Security & Identity
vincent.bouatou@idemia.com



Join us on     

www.idemia.com