Towards an Economic Valuation of Telco-based Identity Management Enablers

PrimeLife/IFIP Summer School 2010

Helsingborg, 2010-08-04

Kai Rannenberg, Sascha Koschinat, Andreas Albers, Gökhan Bal, Marvin Hegen, Christian Weber
T-Mobile Chair of Mobile Business & Multilateral Security
Institute of Business Informatics
Goethe University Frankfurt
www.m-chair.net

mobile business

Agenda

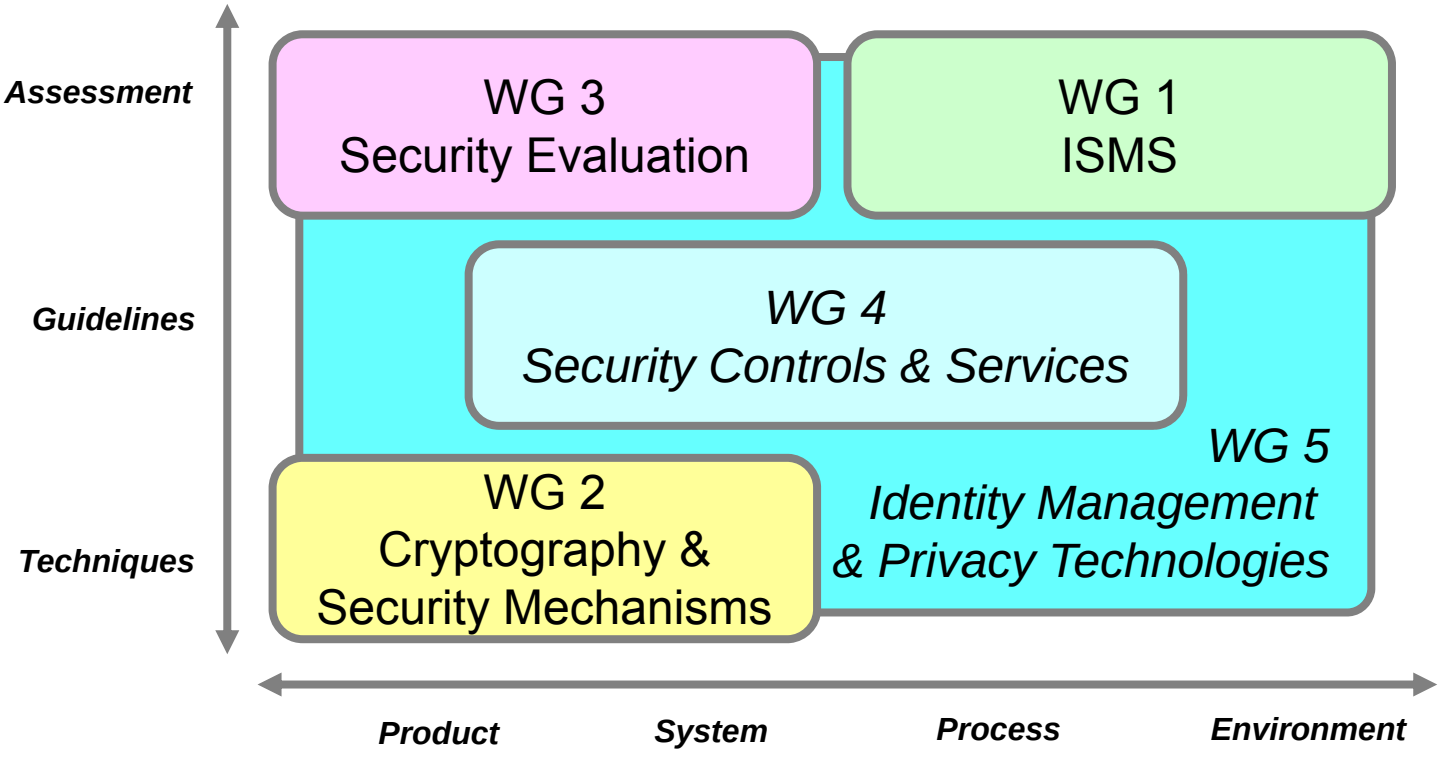
1. Identity Management in ISO/IEC Standardisation
2. Multilateral Security
3. The Identity Management Enabler Concept
4. Motivating the Provision of IdM Enablers by Telecoms
5. Evaluation Approach for IdM Enablers
6. Economic Evaluation of exemplary IdM Enabler "Age Verification"
7. Conclusion and questions for discussion

mobile business

Agenda

1. Identity Management in ISO/IEC JTC 1 Standardisation
2. Multilateral Security
3. The Identity Management Enabler Concept
4. Motivating the Provision of IdM Enablers by Telecoms
5. Evaluation Approach for IdM Enablers
6. Economic Evaluation of exemplary IdM Enabler "Age Verification"
7. Conclusion and questions for discussion

WGs within ISO/IEC JTC 1/SC 27 – IT Security Techniques



WG 5 Identity Management & Privacy Technologies History

October 2003

JTC 1 Plenary established

- **JTC 1 Study Group on Privacy Technologies (SGPT)**
- **for one year period of time (until October 2004) to identify standardization needs**

October 2004

JTC 1 Plenary resolved to

- **disband SGPT**
- **assign to SC 27 further activities in the Privacy Technologies area such as**
  - **a further inventory**
  - **a report back to the November 2006 JTC 1 Plenary**

WG 5 Identity Management & Privacy Technologies History

SC 27 activities (in response to JTC 1's request from October 2004)

- October 2004
  - Study Period on Identity Management established
- May 2005
  - Study Period on Privacy established
  - New Work Item Proposal: A framework for identity management (ISO/IEC 24760)
- May 2006
  - New Working Group 5 on Identity Management and Privacy Technologies established
  - Two new Work Item Proposals
    - A privacy framework (ISO/IEC 29100)
    - A privacy reference architecture (ISO/IEC 29101)

Identity Management (IdM)
An early approach

- „Fear not, for I have redeemed you;
  I have called you by name: you are mine."
  [Isaiah 43:1]

- „Μη φοβου· διοτι εγω σε ελυτρωσα,
  σε εκαλεσα με το ονομα σου· εμου εισαι"
  [Ησαιαν 43:1]

- „No temas, porque yo te he redimido,
  te he llamado por tu nombre; mío eres tú."
  [Isaías 43 [1]]

- „Fürchte dich nicht, denn ich habe dich erlöst;
  ich habe dich bei deinem Namen gerufen; du bist mein!"
  [Jesaja 43,1]

Identity Management (IdM)
2 sides of a medal with enormous economic potential

- **Organisations** aim to sort out
  - User Accounts in different IT systems
  - Authentication
  - Rights management
  - Access control
- **Unified identities** help to
  - ease administration
  - manage customer relations
- **Identity management systems**
  - ease single-sign-on by unify accounts
  - solve the problems of multiple passwords

- **People** live their life
  - in different roles (professional, private, volunteer)
  - using different identities (pseudonyms): email accounts, SIM cards, eBay trade names, chat names, 2ndLife names, …)
- **Differentiated identities** help to
  - protect
    - privacy, especially anonymity
    - personal security/safety
  - enable reputation building at the same time
- **Identity management systems**
  - support users using role based identities
  - help to present the “right” identity in the right context

Identity Management (IdM)
2 sides of a medal with enormous economic potential

- **People** live their life
  - in different roles (professional, private, volunteer)
  - using different identities (pseudonyms): email accounts, SIM cards, eBay trade names, chat names, 2ndLife names, …)
- **Differentiated identities** help to
  - protect
    - privacy, especially anonymity
    - personal security/safety
  - enable reputation building at the same time
- **Identity management systems**
  - support users using role based identities
  - help to present the “right” identity in the right context

- **Organisations** aim to sort out
  - User Accounts in different IT systems
  - Authentication
  - Rights management
  - Access control
- **Unified identities** help to
  - ease administration
  - manage customer relations
- **Identity management systems**
  - ease single-sign-on by unify accounts
  - solve the problems of multiple passwords

WG 5 Identity Management & Privacy Technologies Scope

- Development and maintenance of standards and guidelines addressing security aspects of
  - Identity management
  - Biometrics and
  - Privacy

WG 5 Identity Management & Privacy Technologies Programme of Work

Frameworks & Architectures

- A Framework for Identity Management (ISO/IEC 24760, CD)
- Privacy Framework (ISO/IEC 29100, CD)
- Privacy Reference Architecture (ISO/IEC 29101, CD)
- Entity Authentication Assurance Framework (ISO/IEC 29115 / ITU-T X.eaa, CD)
- A Framework for Access Management (ISO/IEC 29146, WD)

Protection Concepts

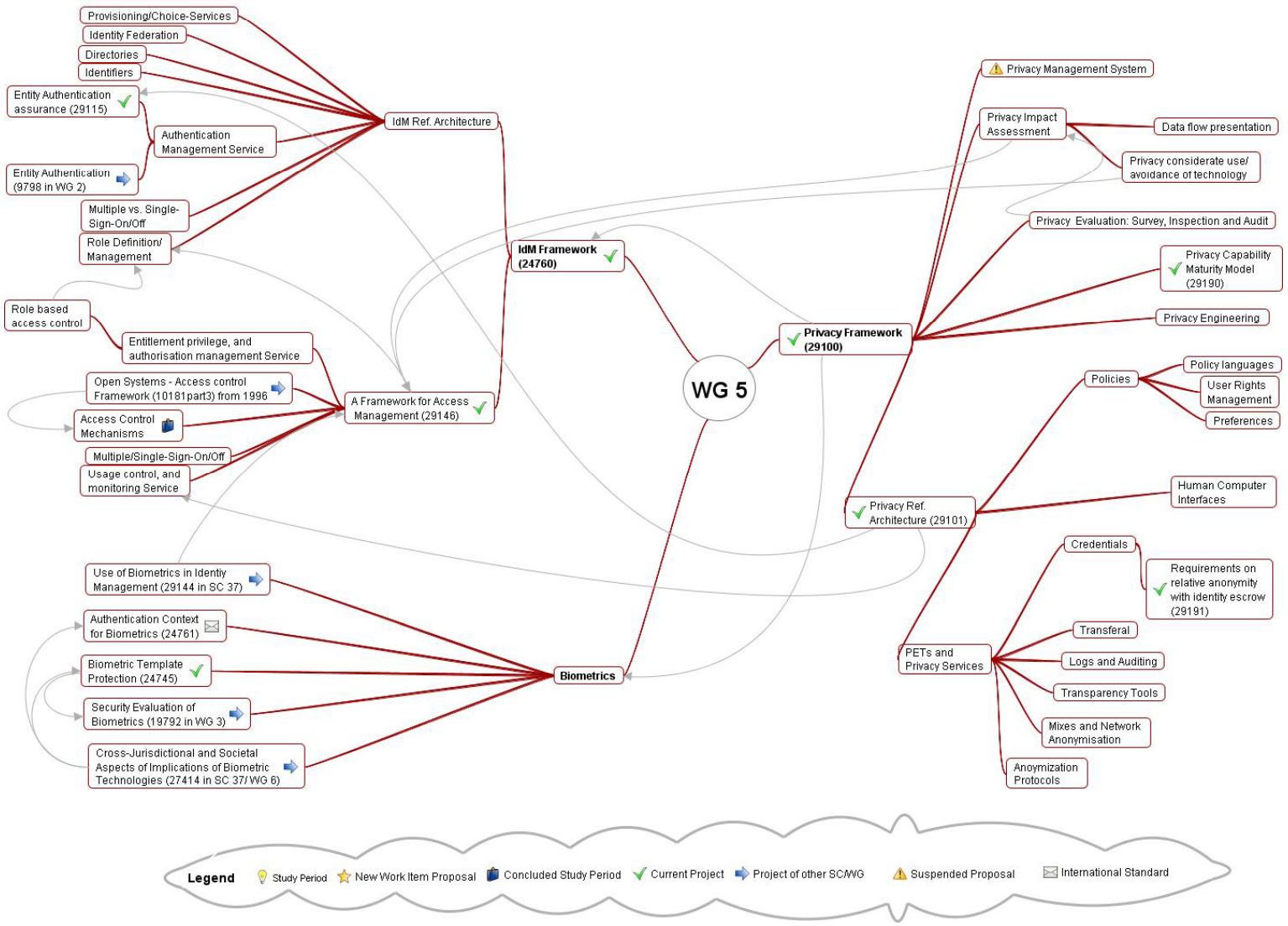
- Biometric information protection (ISO/IEC 24745, FCD)
- Requirements on relative anonymity with identity escrow – model for authentication and authorization using group signatures (ISO/IEC 29191, WD)

Guidance on Context and Assessment

- Authentication Context for Biometrics (ISO/IEC 24761, IS)
- Privacy Capability Assessment Model (ISO/IEC 29190, WD)

WG 5 Identity Management & Privacy Technologies Roadmap

ISO/IEC JTC 1/SC 27/WG 5 Identity Management & Privacy Technologies

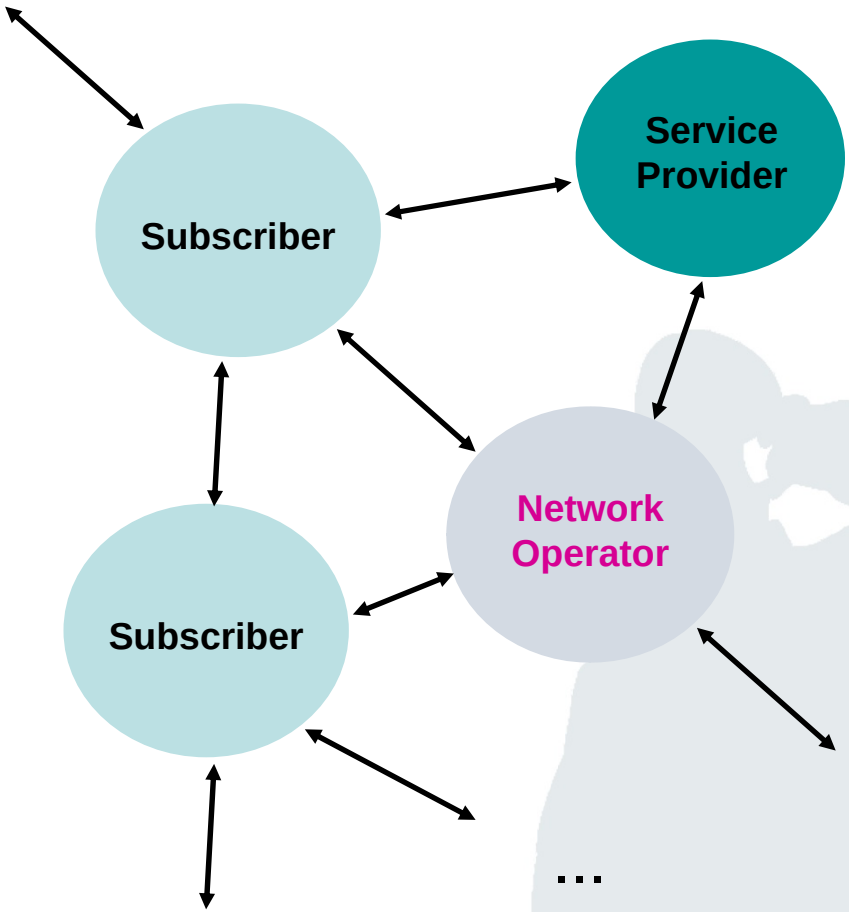


mobile business

Agenda

1. Identity Management in ISO/IEC Standardisation
2. Multilateral Security
3. The Identity Management Enabler Concept
4. Motivating the Provision of IdM Enablers by Telecoms
5. Evaluation Approach for IdM Enablers
6. Economic Evaluation of exemplary IdM Enabler "Age Verification"
7. Conclusion and questions for discussion

Different parties with different interests in communication networks



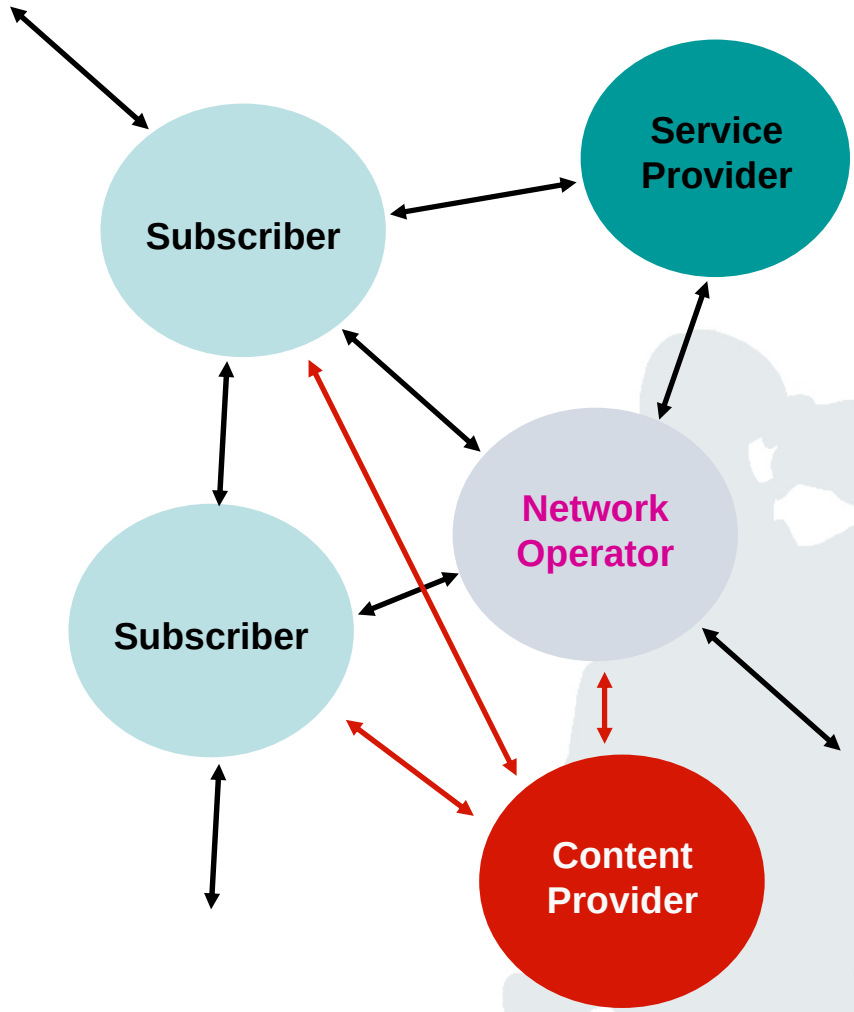
Other examples

- Customers/ Merchants
- Communication partners
- Citizens/ Administration

… in E/M-commerce

… in a world of consortia

- more partners
- more complex relations



Multilateral Security

Respecting Interests

Supporting Sovereignty

Protection of different parties and their interests

Considering Conflicts

Multilateral Security considers conflicts

Respecting Interests

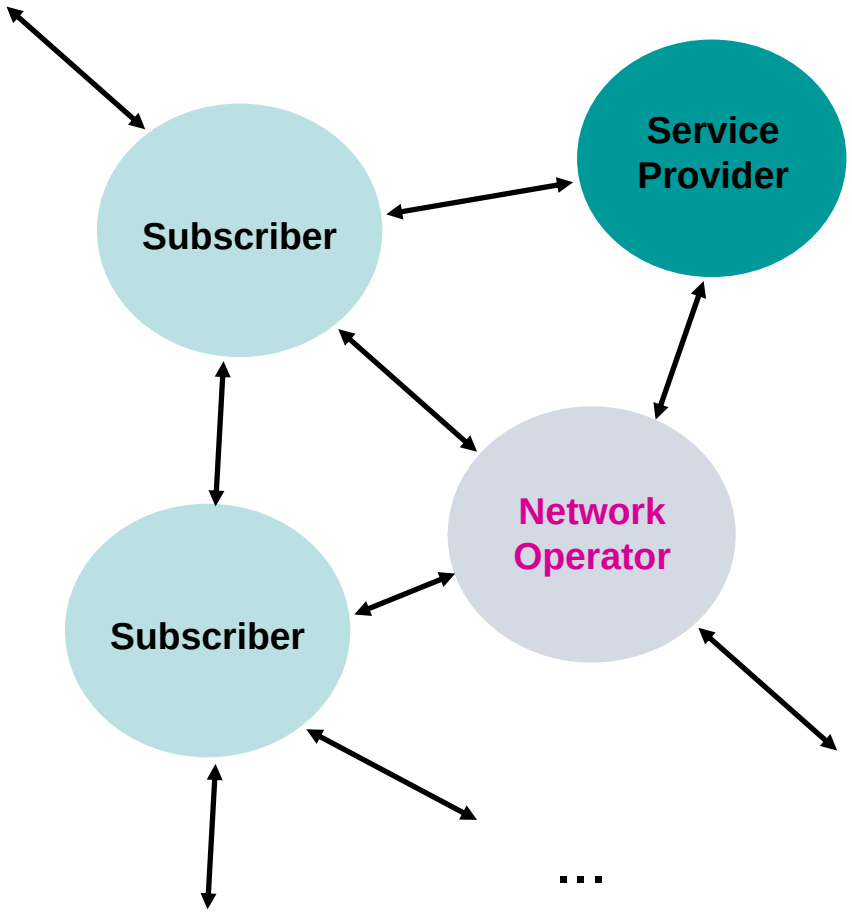
- Parties can define their own **interests**.
- Conflicts can be **recognised** and **negotiated**.
- Negotiated **results** can be reliably **enforced**.

Supporting Sovereignty

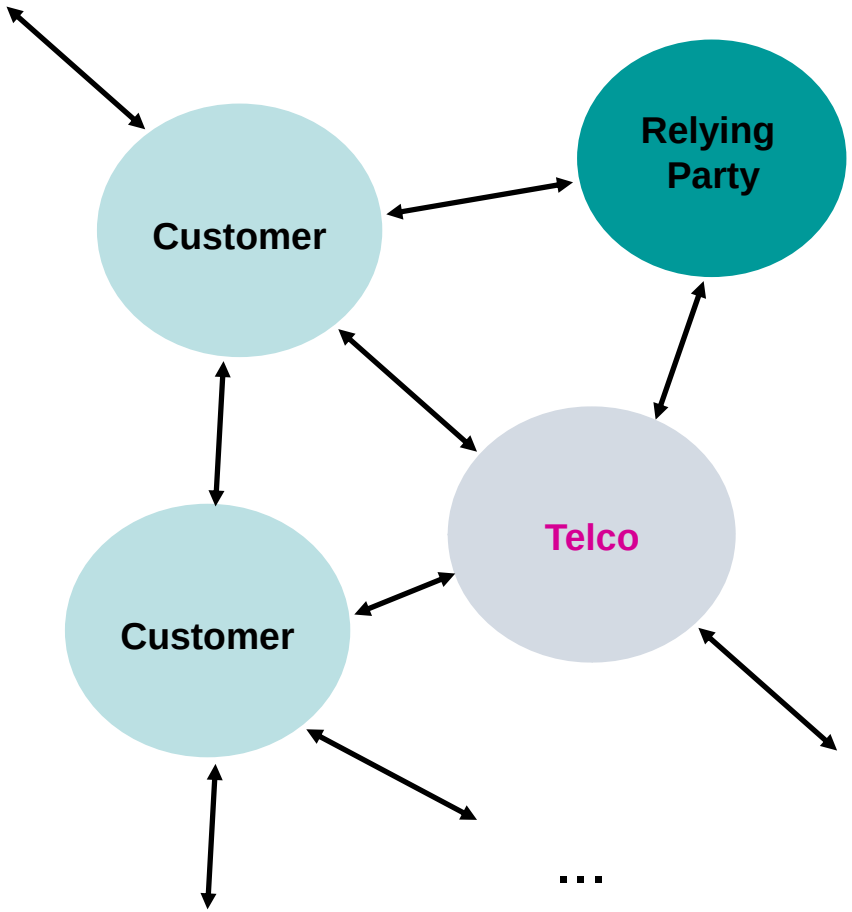
- Requiring each party to **only minimally trust** in the honesty of **others**
- Requiring **only minimal or no trust in technology** of others

Protection of **different parties** and their **interests**

A simplified model for this presentation



Bringing terms closer to the IdM world of terms



mobile business

Agenda

1. Identity Management in ISO/IEC Standardisation
2. Multilateral Security
3. The Identity Management Enabler Concept
4. Motivating the Provision of IdM Enablers by Telecoms
5. Evaluation Approach for IdM Enablers
6. Economic Evaluation of exemplary IdM Enabler "Age Verification"
7. Conclusion and questions for discussion

The Identity Management Enabler Concept

Problem Statement

- Typical problem areas in transactions between businesses and consumers, and governments and citizens:
  - authenticating users
  - validating authorisations
  - market research activities
  - targeting promotions
  - …
- Customer data is processed by various parties and in various ways.
- The involved Identity Management (IdM) processes:
  - are often slow, inefficient and ineffective
  - waste money and affect customer satisfaction
  - often create privacy, security and trust issues
  - …

The Identity Management Enabler Concept

Motivation

- A potential for enabling new added values lies in addressing this situation by:
  - providing required personal data of consumers or citizen **(IdM Assets)** to their transaction partners (businesses and governments)
  - automatic processing of personal data by technical functions **(IdM Capabilities)** under legal, compliance, and personal requirements
  - consistent and coherent combinations of IdM Assets and IdM Capabilities for each transaction **(IdM Enablers)** to enable and enhance the respective IdM processes
  - a trusted **IdM Service Provider** that can (with minimal effort) provide the transactions partners with adequate IdM Enablers
- This concept here is called IdM Enabler Concept.

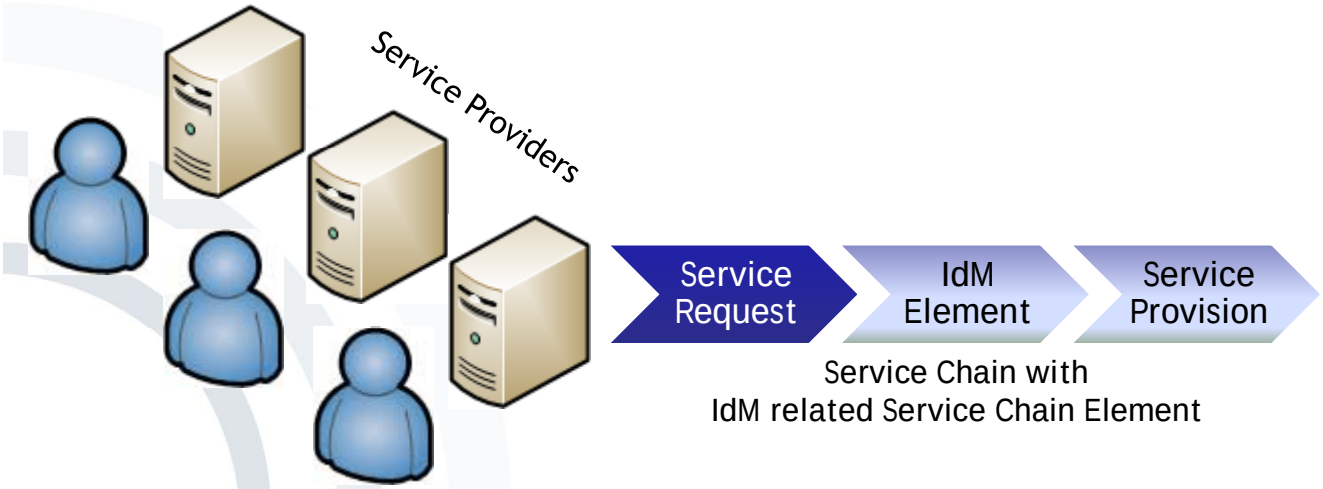
The Identity Management Enabler Concept

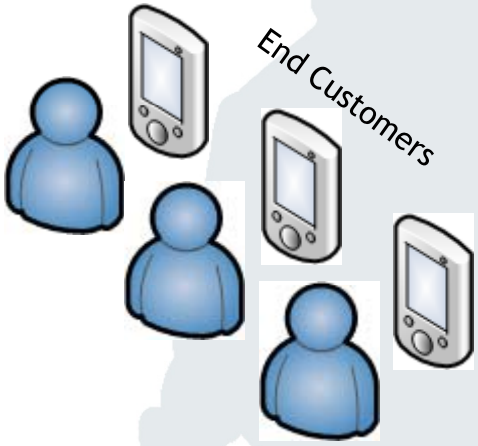
Objectives

- The IdM Enabler Concept has emerged to:
  - illustrate the importance of IdM processes in everyday business transactions
  - structure relevant IdM components for business transactions
  - valuate different options of IdM enhanced business transactions
- The following simple example „Age Verification“ shall illustrate some of these implications.

The Identity Management Enabler Concept

Internet Service Value Chain





The Identity Management Enabler Concept

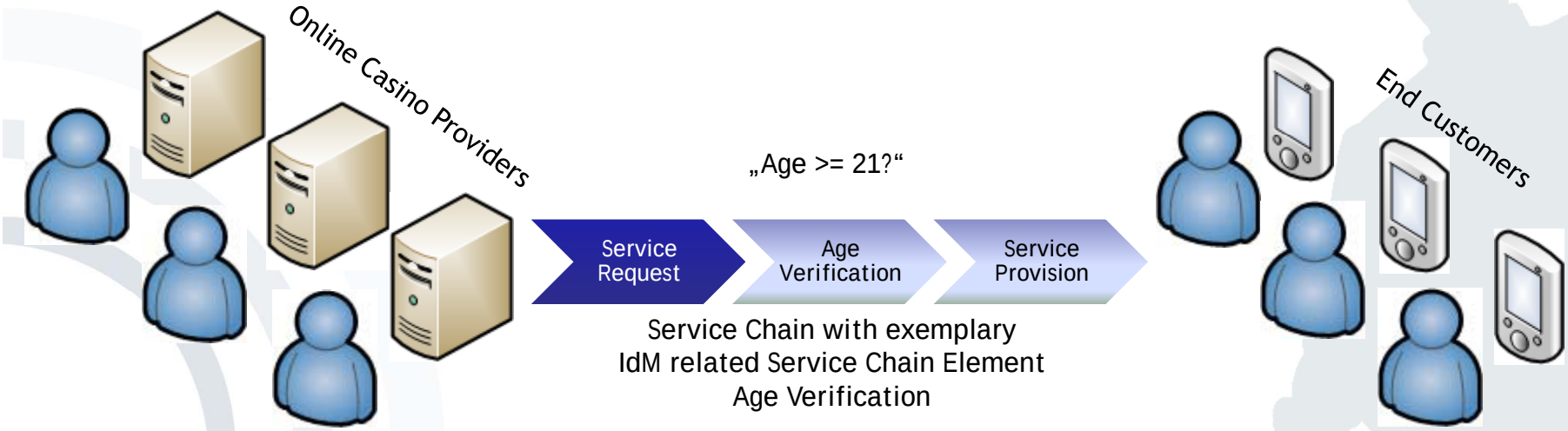
Example - Age Verification

Service Providers' problems:

- Payment Enforcement
- Compliance
- …

End Customers' problems:

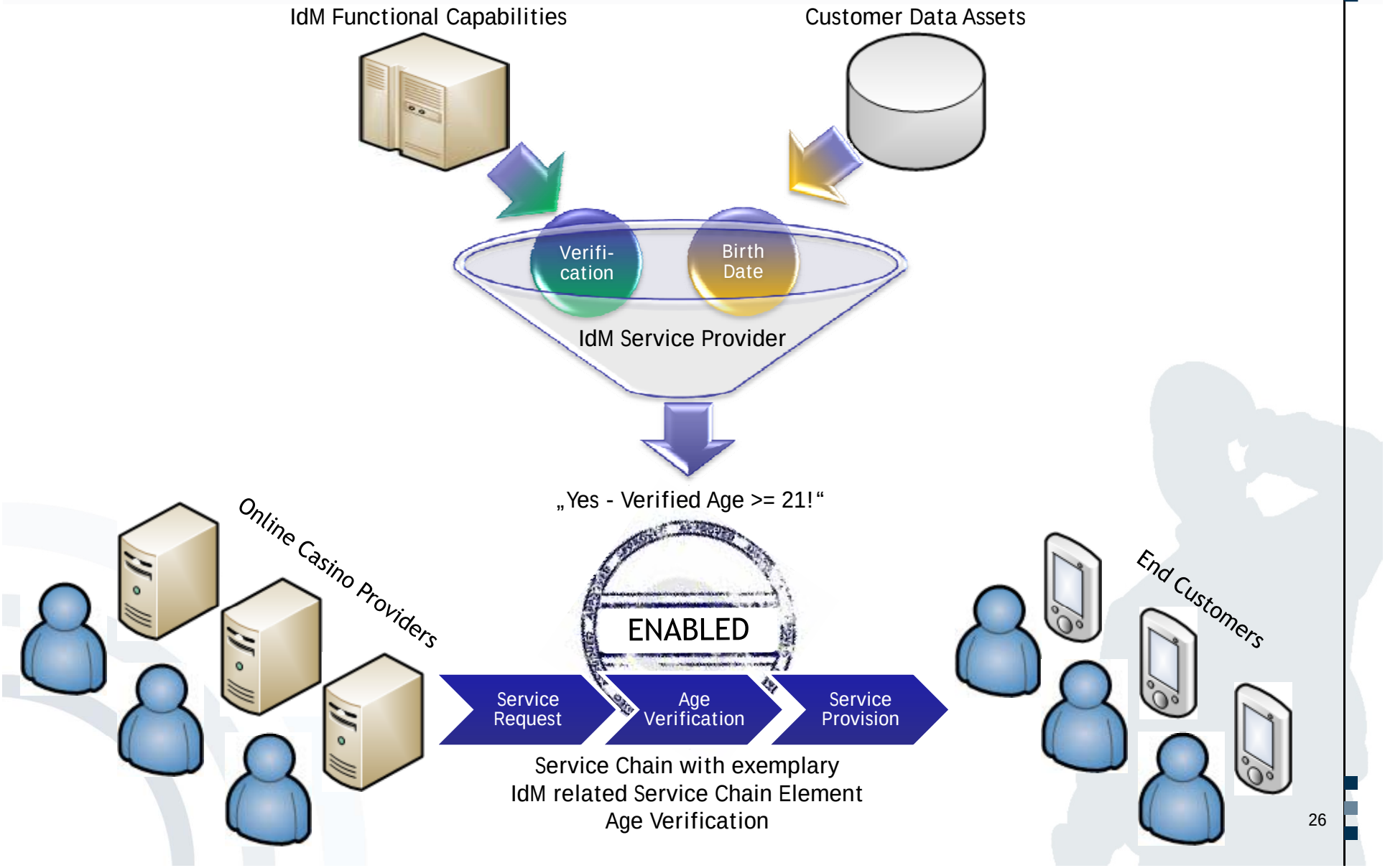
- Convenience/Usability
- Risk of data misuse
- …



Service Chain with exemplary IdM related Service Chain Element Age Verification

The Identity Management Enabler Concept

Example - Age Verification

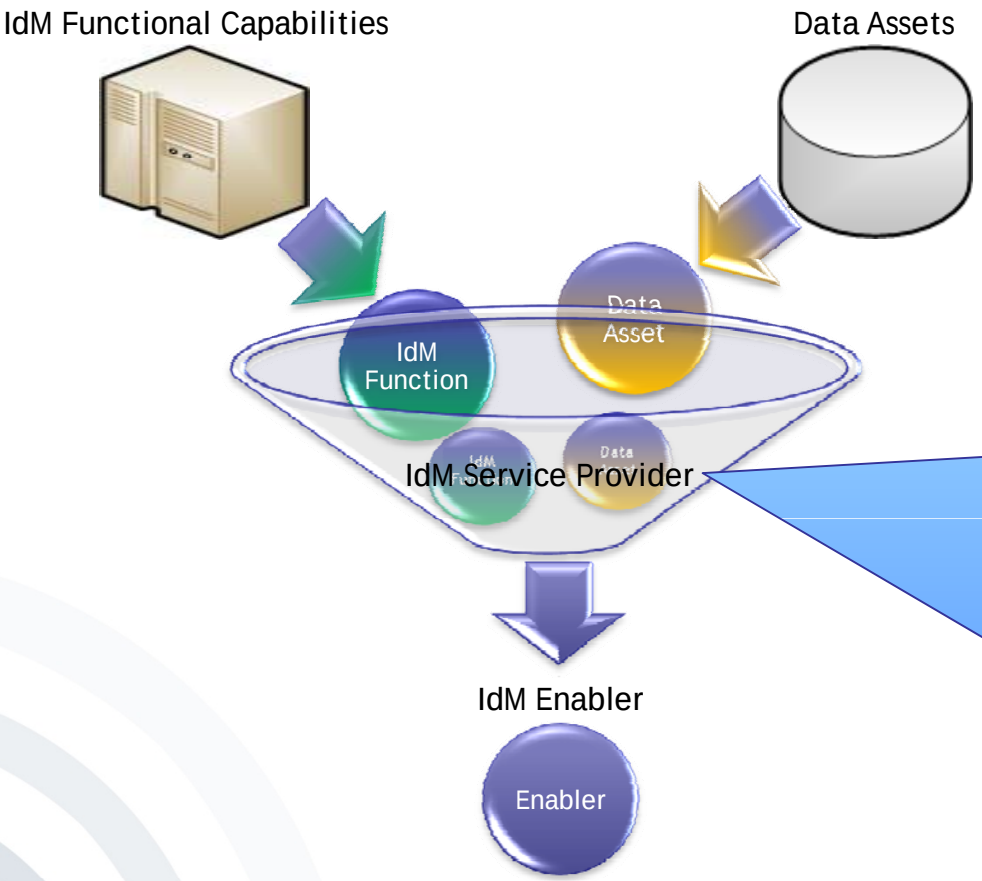


mobile business

Agenda

1. Identity Management in ISO/IEC Standardisation
2. Multilateral Security
3. The Identity Management Enabler Concept
4. Motivating the Provision of IdM Enablers by Telecoms
5. Evaluation Approach for IdM Enablers
6. Economic Evaluation of exemplary IdM Enabler "Age Verification"
7. Conclusion and questions for discussion

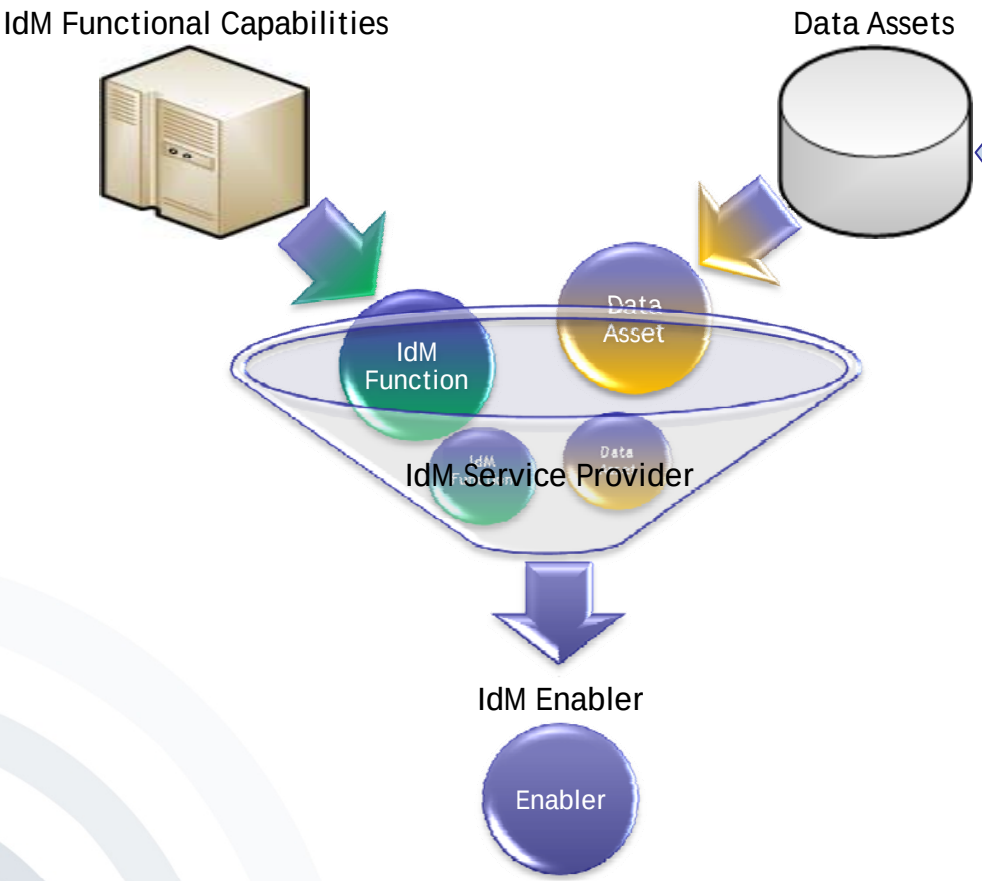
Motivating Telcos as IdM Service Providers



Who could be in the role of providing IdM Enablers for business transactions between End Customers and Service Providers?

- No single player
- A Value Network of different IdM Service Providers
- Telcos have a good chance of becoming big players.
- Telcos fulfil essential requirements to enable win-win situations.
- Telcos have more incentives to protect and respect their customers' privacy than other players.
- Focus on Telcos!

IdM Components - Data Assets

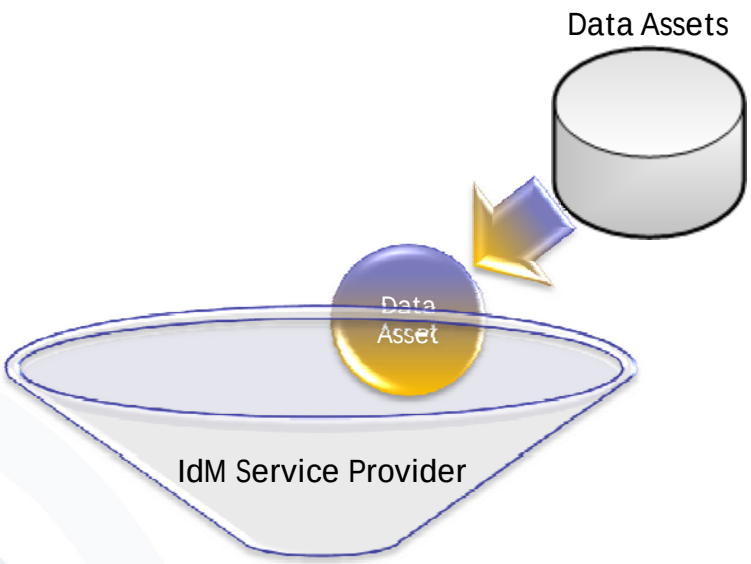


Which Data Assets does a Telco possess?

- They have a lot of customer data.
- Specifically they have even more and more valuable customer data concentrated in their databases than other businesses.
- Catalogue of Telco Data Assets (cf. H6.1.2) and Data Assets of other big players.

Telco Data Assets

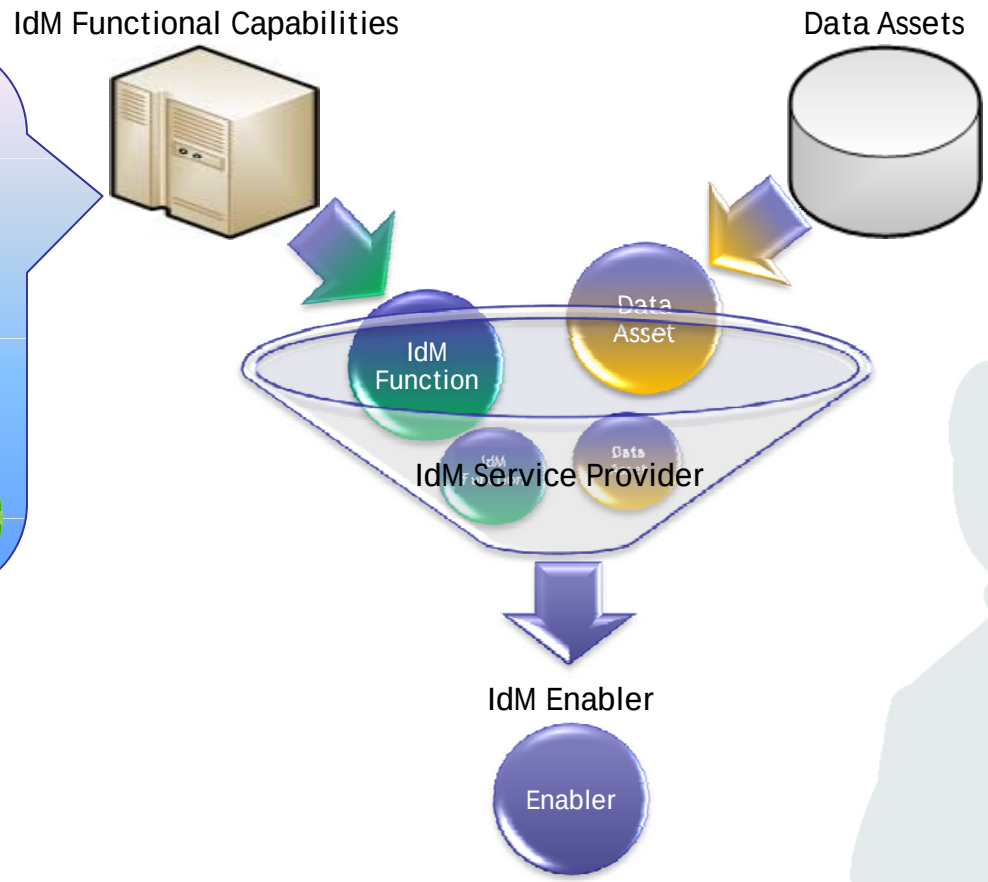
Basic Data	Identification Data	Communication Data	Content Data	Context Data	Financial Data	Device Data
•Name •Address •...	•Username & Password •Phone Number •...	•SMS Detail Record •Call Detail Record •...	•Videos •Blogs •...	•Place •Time •...	• Credit Worthiness •Buying Patterns •...	• Device Type • Battery Status • ...



IdM Components - Functional Capabilities

3. Which IdM Functions can a Telco already provide?

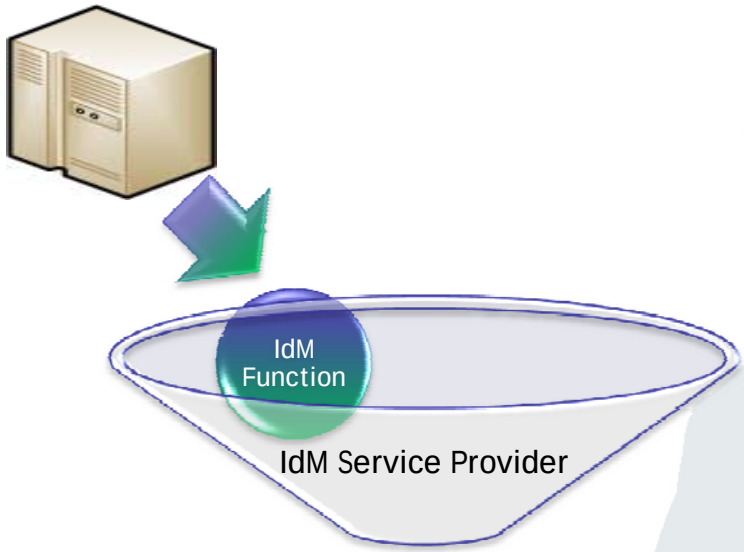
- Telcos already implement a big subset of IdM Functions.
- Telcos fulfil essential requirements to provide their IdM Functions to a wide IdM ecosystem.
- Catalogue of Telco IdM Functions (cf. H6.1.2).



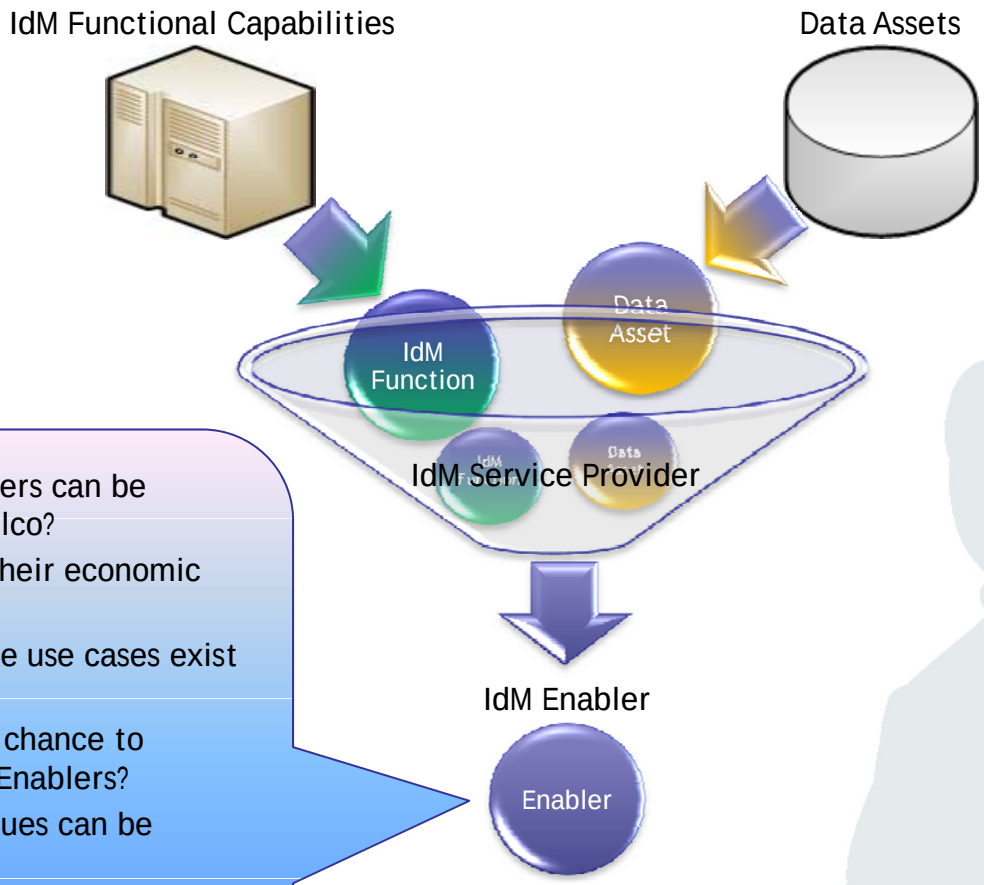
Functional Capabilities of Telcos

Account Functions	Attribute Functions	Authentication Functions	Authorization Functions	Policy Functions
•Federation •Blocking •…	•Verification •Revocation •…	•Authentication •SSO •…	•Authorization •Revoke SignedToken •…	•Editing •Update •…

IdM Functional Capabilities



Economic Evaluation of Telco-based IdM Enablers
Interesting Questions



1. Which IdM Enablers can be provided by a Telco?
2. How obvious is their economic relevance?
3. Which reasonable use cases exist for them?
4. How good is the chance to monetize these Enablers?
5. Which added values can be enabled?
6. How big is their economic potential?

Agenda

1. Identity Management in ISO/IEC Standardisation
2. Multilateral Security
3. The Identity Management Enabler Concept
4. Motivating the Provision of IdM Enablers by Telecoms
5. Evaluation Approach for IdM Enablers
6. Economic Evaluation of exemplary IdM Enabler "Age Verification"
7. Conclusion and questions for discussion

Development process for Economic Evaluation Framework

1. Description of feasible IdM Enabler Service Options
2. Stakeholder identification and description (objectives etc.)
3. Identification and Analysis of the impacts of available IdM Enabler Service Options on the stakeholders
   - Possible impacts: e.g. costs, usability, functionality, ...
   - Evaluation Approach based on Cost Benefit Analysis
4. Identification of Cause-Effect Chains between the stakeholders
5. Cost Benefit Overview from the perspective of the IdM Service Provider
6. Cost Benefit Analysis for IdM Service Provider

Agenda

1. Identity Management in ISO/IEC Standardisation
2. Multilateral Security
3. The Identity Management Enabler Concept
4. Motivating the Provision of IdM Enablers by Telecoms
5. Evaluation Approach for IdM Enablers
6. Economic Evaluation of exemplary IdM Enabler "Age Verification"
7. Conclusion and questions for discussion

mobile business

Options

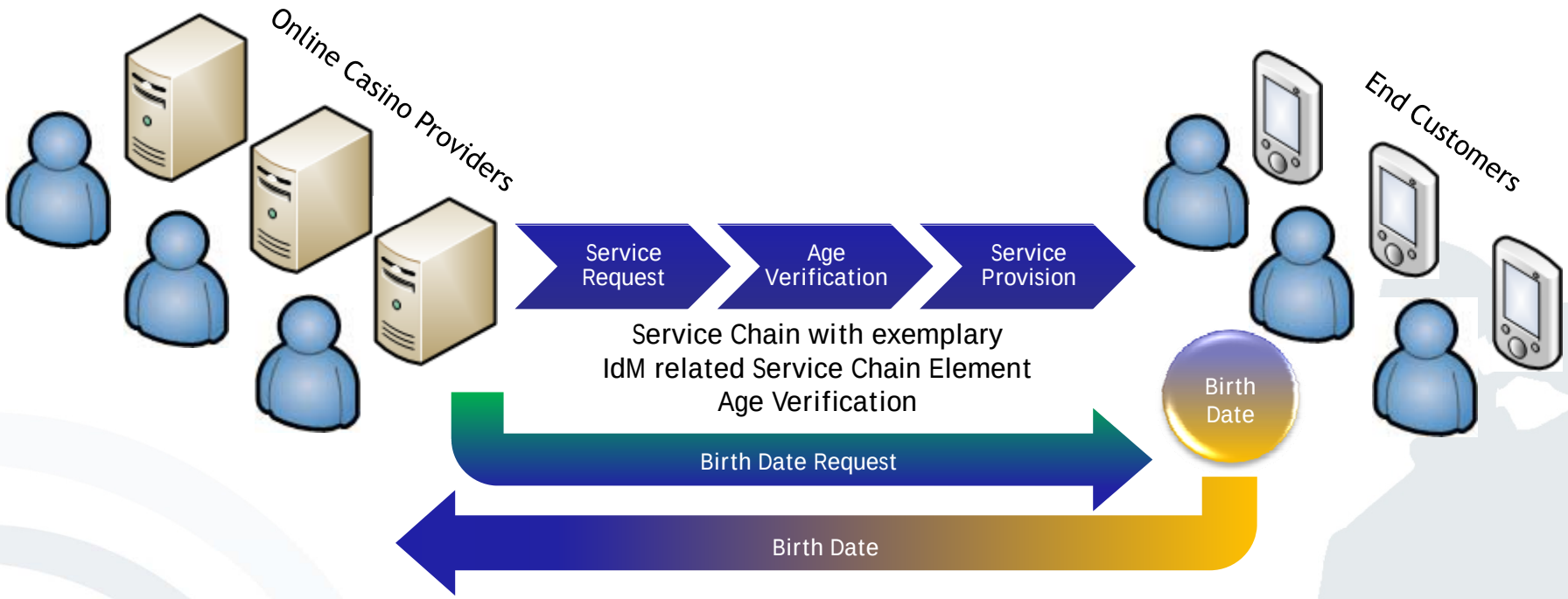
1. Customer provides age information (CPI).

2. Telco provides verified age information certificate to user (TPC).

3. Telco provides verified age information to Service Provider (TPI).

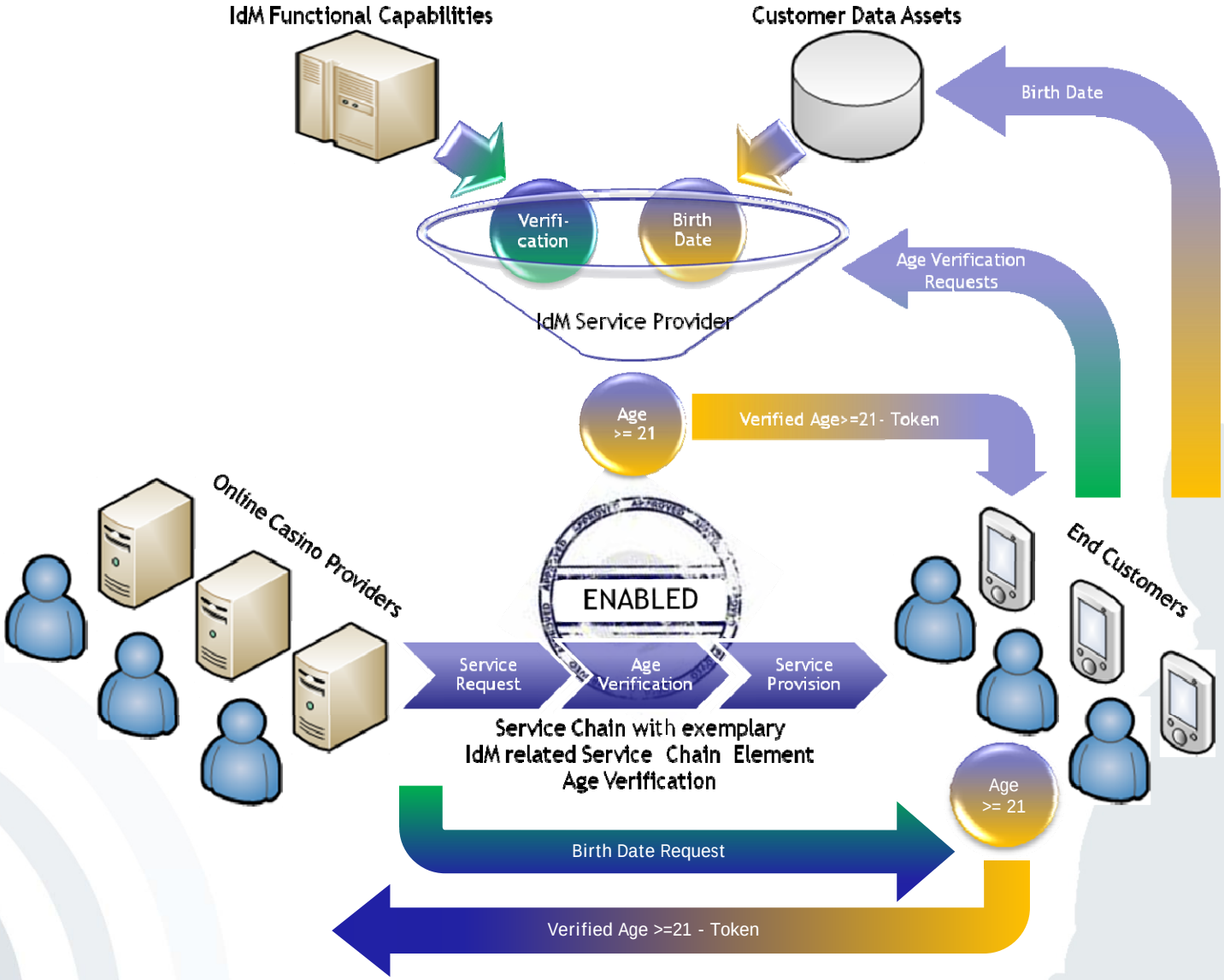
IdM Enabler Service Options

Option 1 (CPI) - Customer provides age information



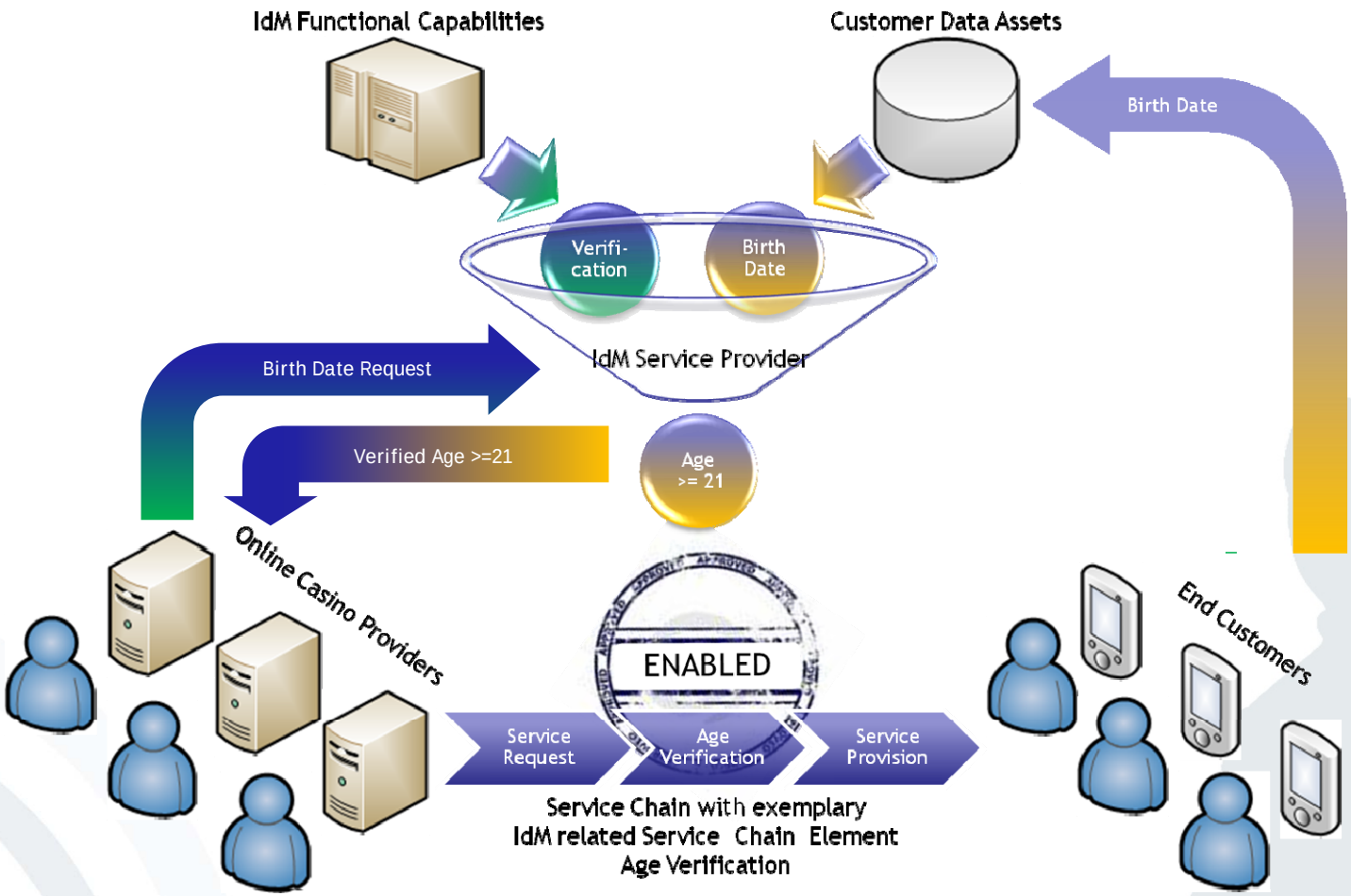
IdM Enabler Service Options

Option 2 (TPC) - Telco provides verified age information certificate to user



IdM Enabler Service Options

Option 3 (TPI) - Telco provides verified age information to Service Provider



Stakeholders and their Objectives

Customer (**using** a service):

- Minimize efforts and risks (registration, data misuse, …)
- Maximize performance and **privacy** (transaction speed, anonymity, …)

Service Provider (**providing** a service):

- Minimize efforts and risks (compliance, payment assurance, …)
- Maximize performance and revenues (customer loyalty, willingness to pay, …)

Telco (providing an **IdM Service**):

- Maximize performance and revenues (brand awareness, retention rate, …)
- Minimize efforts and risks (infrastructure, security , …)

Costs & Benefits
Option 2 (TPC) vs. Option 1 (CPI)
Customer Perspective

Benefits	Costs
Additional Data Minimisation (more Privacy)	**Additional efforts for Hardware and/or Software**
Lower risk of data misuse by Service Providers	Additional efforts for Telco registration
Higher trust in Service Providers (as they demonstrate privacy-friendliness)	**Additional registration fees and/or charges for service usage**
Additional guaranteed compliance with regulation	Higher duration of transactions (possibly one-time for Service Provider registration)
Higher convenience for being compliant with regulation	Additional trust relationship to Telco required / risk of data misuse by Telco
	Additional risk of missing availability of a service due to failure of Customer or Telco infrastructure

Costs & Benefits

Option 2 (TPC) vs. Option 1 (CPI)
Service Provider Perspective

Benefits	Costs
Higher trust/lower risk by Customers → higher customer loyalty → more new customers → more revenues	**Fewer possibilities for commercialization of customer data**
Additional compliance with regulation assured by Telco	**Less information about customers → less potential for advertising, personalisation, profiling, targeting etc.**
Lower risk of payment losses through minors	Additional risk of missing availability of a service due to failure of Customer or Telco infrastructure
Fewer efforts for infrastructure implementation and operation	Higher duration of transactions (possibly one-time for Service Provider registration)
Fewer efforts for Customer support	

Costs & Benefits
Option 2 (TPC) vs. Option 1 (CPI)
Telco Perspective

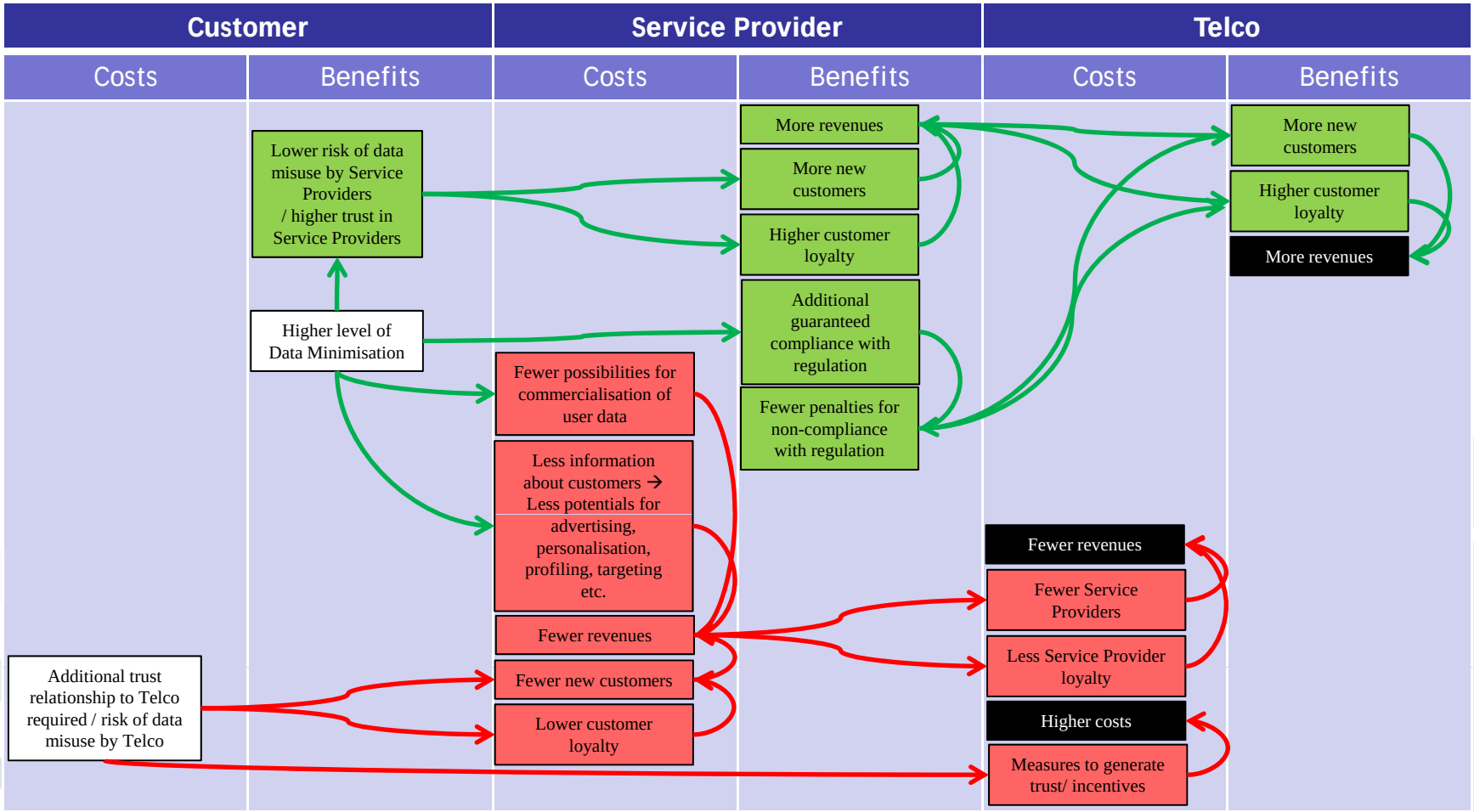
Benefits	Costs
Additional Value Added Service for Customers → Higher Customer loyalty → More new Customers → More revenues	**Additional efforts for development and operation of hardware and/or software for Customers**
Higher market entry barriers for possible business rivals	Additional efforts for development and operation of the Service Infrastructure (data bases, etc.)
	Additional efforts for development and operation of the Business Model (Payment & Billing, critical mass of Customers and Service Providers etc.)
	Additional efforts for correction of incorrect age verifications (liability guarantee for Customers and Service Providers)
	Additional efforts for Customer Support

Consideration of interdependencies by Cause-Effect Chains

- A single stakeholders' costs and benefits have an effect on the other stakeholders' costs and benefits
- When analysing and evaluating the different options these interdependencies need to be considered
- Cause-Effect Chains can help to reflect the interdependencies between the stakeholders' costs and benefits
- In the following, the Cause-Effect Chains for selected Customers' costs and benefits of Option 2 (TPC) vs. Option 1 (CPI) will be presented in order to reflect their effect on the other stakeholders' costs and benefits
- Selected Customers' costs and benefits:
  - Higher level of data minimisation (more Privacy)
  - Additional trust relationship to Telco required (additional risk of data misuse by Telco)

Cause-Effect Chain for selected Costs & Benefits

Option 2 (TPC) vs. Option 1 (CPI)



Stakeholders and their Objectives (revisited)

Customer (**using** a service):

- Minimize efforts and risks (registration, data misuse, …)
- Maximize performance and **privacy** (transaction speed, anonymity, …)

Service Provider (**providing** a service):

- Minimize efforts and risks (compliance, payment assurance, …)
- Maximize performance and revenues (customer loyalty, willingness to pay, …)

Telco (providing an **IdM Service**):

- Maximize performance and revenues (brand awareness, retention rate, …)
- Minimize efforts and risks (infrastructure, security , …)

Effects on Stakeholders' Objectives

Option 2 (TPC) vs. Option 1 (CPI)

Customer:

- Additional efforts (service usage, hardware/software)
- Lower risks in relationship to Service Providers (trust, data misuse)
- Additional risks in relationship to Telco (trust, availability)
- More performance in service usage (convenience, compliance)
- Less performance in service usage (transaction duration, registration)
- More Privacy-friendly transactions (data minimisation, privacy)

Service Provider:

- Lower efforts (infrastructure, support)
- Lower risks with respect to Customer and regulations (compliance, payment losses)
- Additional risks of Customer and Telco infrastructure (availability, trust)
- More revenues (customer loyalty, new customers)
- Fewer revenues (customer data, advertising)

Telco:

- More revenues (customer loyalty, new customers)
- Additional efforts (software/hardware for Customers, Service Provider incentives, infrastructure)

Costs & Benefits
Option 3 (TPI) vs. Option 1 (CPI)
Customer Perspective

Benefits	Costs
Additional Data Minimisation (more Privacy)	**Less Privacy, because of additional knowledge of Telco about Customers‘ Service Providers and additional knowledge of Service Providers about Customers` Telco**
Lower risk of data misuse by Service Providers	Additional efforts for Telco registration
Higher trust in Service Providers	Higher duration of transactions (possibly one-time for Service Provider registration)
Additional guaranteed compliance with regulation	Additional trust relationship to Telco required / Additional risk of data misuse by Telco
Higher convenience for being compliant with regulation	Additional risk of missing availability of a service due to failrure of Telco infrastructure
	Less control about personal data provision / Bigger knowledge about business relationships by Service Provider and Telco (less Privacy)

Costs & Benefits
Option 3 (TPI) vs. Option 1 (CPI)
Service Provider Perspective

Benefits	Costs
More trust by Customers → higher customer loyalty → more new customers → more revenues	Fewer possibilities for commercialization of customer data
Additional compliance with regulation assured by Telco	Less information about customers → Less potentials for advertising, personalisation, profiling, targeting etc.
Lower risk of payment losses through minors	Higher duration of transactions (possibly one-time for Service Provider registration)
Fewer efforts for infrastructure implementation and operation	**Additional costs for implementation and operation of interface infrastructure to Telco**
Fewer efforts for Customer support	**Additional registration fees and/or charges for service usage**
Additional business relationship to Telco → additional possibility for new Marketing & Sales-channel → customer base of Telco	Additional risk of missing availability of a service due to failure of Telco infrastructure
	Additional efforts to provide incentives for customers

Costs & Benefits
Option 3 (TPI) vs. Option 1 (CPI) 1
Telco Perspective

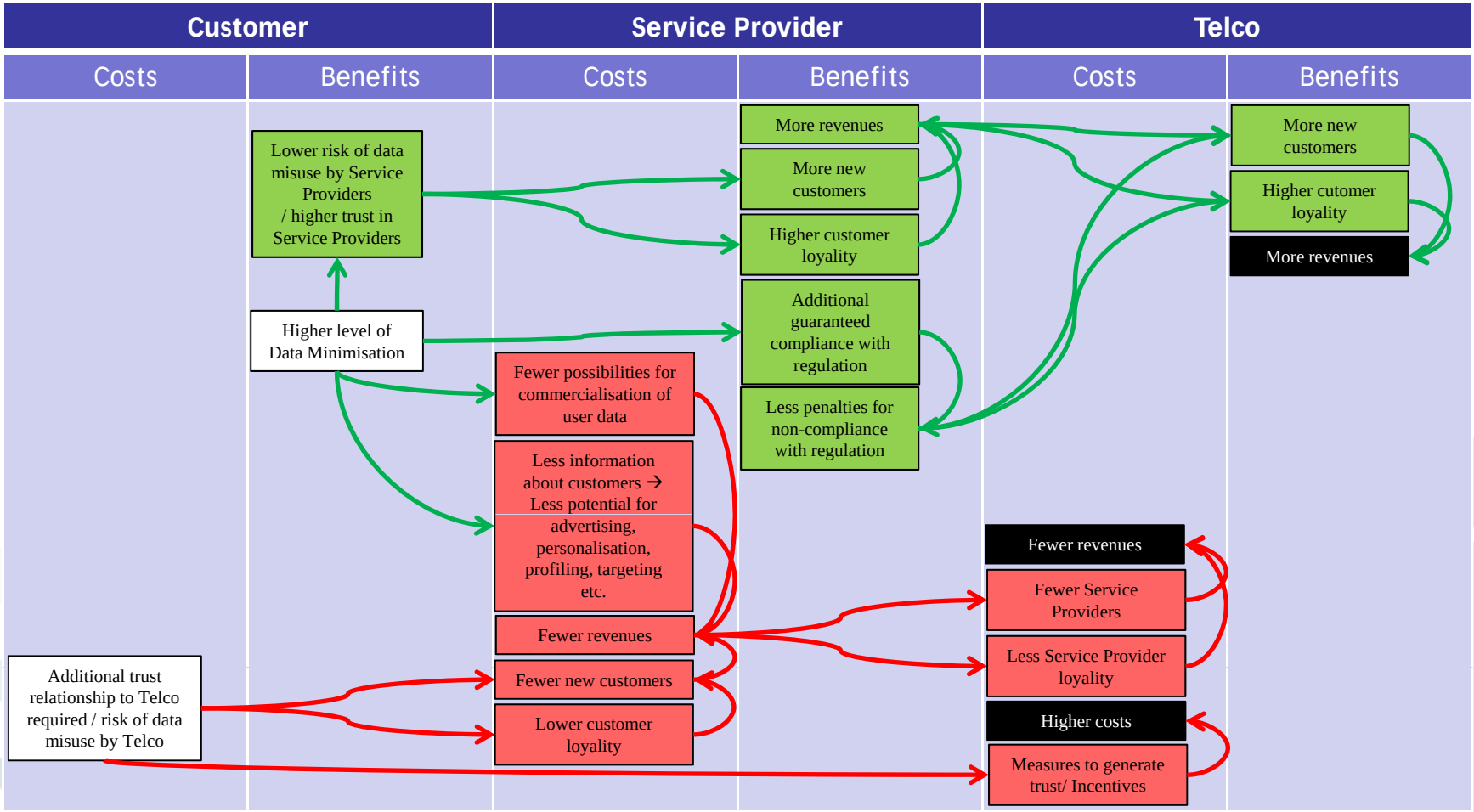
Benefits	Costs
Additional Value Added Service for Customers and Service Providers → Higher customer loyalty → More new customers →More revenues	Additional efforts for development and operation of the Service Infrastructure (data bases, Service Provider Interface etc.)
Additional business relationships to Service Providers → additional possibility for new Marketing & Sales-channels → customer base of Service Providers	Additional efforts for development and operation of the Business Model (Payment & Billing, critical mass of Customers and Service Providers etc.)
Higher market entry barriers for possible business rivals	Additional efforts for correction of incorrect age verifications (liability guarantee for Users and Service Providers)
	Additional efforts for Customer Support

Consideration of interdependencies by Cause-Effect Chains

- In the following, the Cause-Effect Chains for Option 3 (TPI) vs. Option 1 (CPI) will be presented
  - … using the same selected Customers' costs and benefits as for Option 2 (TPC) vs. Option 1 (CPI) before
  - … in order to find possible differences in the Cause-Effect Chains of each option
- Selected Customers' costs and benefits:
  - Higher level of data minimisation (more Privacy)
  - Additional trust relationship to Telco required (additional risk of data misuse by Telco)

Cause-Effect Chain for selected Costs & Benefits

Option 3 (TPI) vs. Option 1 (CPI)



Stakeholders and their Objectives (revisited)

Customer (**using** a service):

- Minimize efforts and risks (registration, data misuse, …)
- Maximize performance and **privacy** (transaction speed, anonymity, …)

Service Provider (**providing** a service):

- Minimize efforts and risks (compliance, payment assurance, …)
- Maximize performance and revenues (customer loyalty, willingness to pay, …)

Telco (providing an **IdM Service**):

- Maximize performance and revenues (brand awareness, retention rate, …)
- Minimize efforts and risks (infrastructure, security , …)

Effects on Stakeholders' Objectives

Option 3 (TPI) vs. Option 1 (CPI)

Customer:

- Lower risks in relationship to Service Providers (trust)
- Additional risks in relationship to Telco (trust, availability)
- More performance for consumption (convenience, compliance)
- More Privacy-friendly transactions (data minimisation)
- Less Privacy-friendly transactions (knowledge about relationships, personal data control)

Service Provider:

- Lower efforts (infrastructure, support)
- Additional efforts (interface, service usage)
- Lower risks (compliance, payment losses)
- Additional risks (availability)
- Less performance for service provision (transaction duration, registration)
- More revenues (customer loyalty, new customers, Telco customer base)
- Fewer revenues (customer data, advertising)

Telco:

- More revenues (Service Provider customer base, customer loyalty, new customers)
- Additional efforts (interface to Service Provider, Service Provider incentives, infrastructure)

Selected Results

Option 3 (TPI) vs. Option 2 (TPC)

- In comparison to Option 1 (CPI), Option 2 (TPC) and Option 3 (TPI) lead to approximately the same costs and benefits.
- But, the slight differences can have an enormous impact on the advantageousness of each option.
- Example:
  - **Option 2 (TPC):** The Telco needs to afford the development, implementation, and operation of the service infrastructure that the **Customer** requires (hardware, software).
  - **Option 3 (TPI) :** The Telco needs to afford the development, implementation, and operation of the service infrastructure that the **Service Provider** requires (online interface).

Selected Results

Option 3 (TPI) vs. Option 2 (TPC)

- Also the Cause-Effect Chains for the selected costs and benefits of Option 2 (TPC) and Option 3 (TPI) lead to approximately the same results
- Differences can only be seen in <u>concrete values</u> of the costs and benefits.
- Example:
  - In comparison of Option 2 (TPC) to Option 3 (TPI) the Customer's risk of a data misuse by the Telco seems to be lower, because of additional possibilities to control the personal data flow.
- The advantages of an option can only be investigated by more sophisticated evaluation methods and more concrete option scenarios.
- Also the use of methods beyond qualitative evaluation methods (e.g. quantitative ones) needs to be considered because of the often quantitative costs and benefits.

mobile business

Agenda

1. Identity Management in ISO/IEC Standardisation
2. Multilateral Security
3. The Identity Management Enabler Concept
4. Motivating the Provision of IdM Enablers by Telecoms
5. Evaluation Approach for IdM Enablers
6. Economic Evaluation of exemplary IdM Enabler "Age Verification"
7. Conclusion and questions for discussion

Conclusion and questions for discussion

- Cost Benefit Analysis and Cause-Effect Chains are an initial evaluation approach.
  - Maybe every enabler needs its own analysis framework.
  - Hopefully we can identify classes of enablers, which can be analyzed with the same analysis framework.

- Next steps
  - Analysing a more detailed scenario using the outlined method
  - Trying out other methods

- Questions for discussion
  - Which aspects influence the economic reasonability and technical feasibility?
  - Are there other promising methods?
  - Are there other cause-effect relations?

References

- Kim Cameron, Reinhard Posch, Kai Rannenberg: Proposal for a common identity framework: A User-Centric Identity Metasystem
- FIDIS: Future of Identity in the Information Society; www.fidis.net
- FIDIS Deliverable 3.6: Study on ID Documents; 2006; www.fidis.net
- ISO/IEC JTC 1/SC 27/WG 5: Identity Management and Privacy Technologies; www.jtc1sc27.din.de
- PICOS: Privacy and Identity Management for Community Services; www.picos-project.eu
- PRIME: Privacy and Identity Management for Europe; www.prime-project.eu
- PrimeLife: Privacy and Identity Management for Life; www.primelife.eu
- Kai Rannenberg: Multilateral Security – A concept and examples for balanced security; Pp. 151-162 in: Proceedings of the 9th ACM New Security Paradigms Workshop 2000, September 19-21, 2000 Cork, Ireland; ACM Press; ISBN 1-58113-260-3
- Kai Rannenberg: Identity management in mobile cellular networks and related applications; Information Security Technical Report; Vol. 9, No. 1; 2004; pp. 77 – 85; ISSN 1363-4127
- T-Mobile Chair for Mobile Business & Multilateral Security @ Goethe University Frankfurt; www.m-chair-net