



**Rabobank**

# The key(s) to always access

## 14th SAFE-NL workshop

Rob Heijjer MSc, CISSP  
Security manager

Rabobank Nederland  
GroepICT – ICT Beleid en Architectuur  
[r.c.heijjer@rn.rabobank.nl](mailto:r.c.heijjer@rn.rabobank.nl)

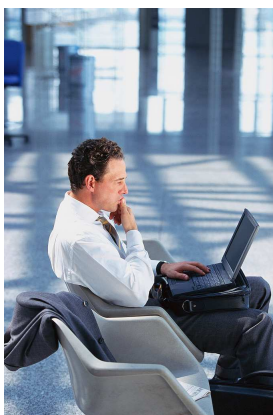
December 12 - 2008

Any time, any place, anywhere ...



Rabobank

is not a problem anymore

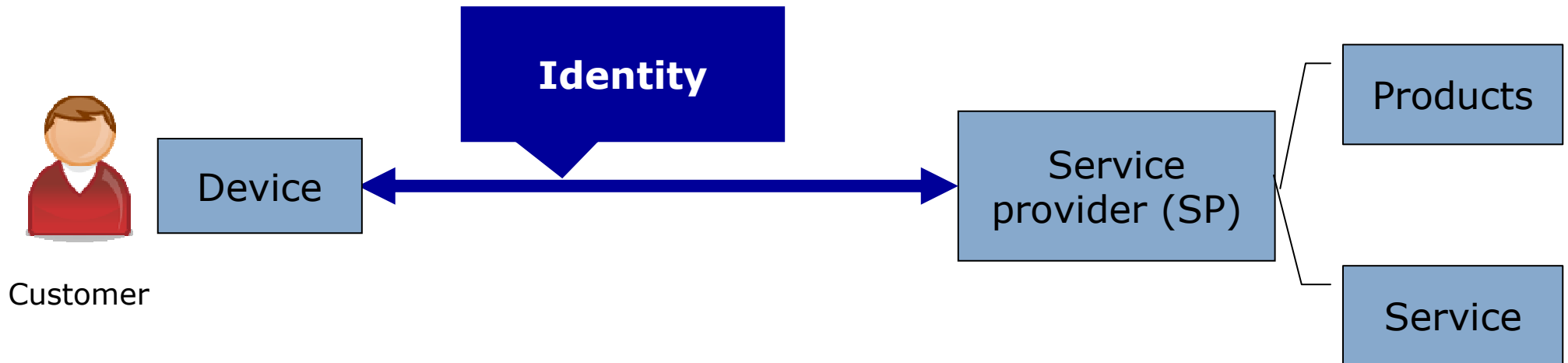


A collection of various keys scattered on a light-colored surface. The keys are of different shapes and sizes, including a large brass key with a handle, a silver key with a handle, and several smaller keys. The text "Always access is the problem" is overlaid on the image in a blue font.

Always access is the problem

do I have my (access) key(s) with me?

# Introduction



"The value of identity of course is that so often with it comes purpose."

Richard R. Grant

# Service provisioning



**Rabobank**

- User friendly = Convenience
  - Market acceptance
  - Features
  - Operation
  
- Risks
  - Financial damage
  - Reputational damage
  
- Level of service = Authorisation
  - Assurance of identity +
  - Assurance of authentication (process, security) +
  - Convenience +
  - Risk balance (risk analyses)

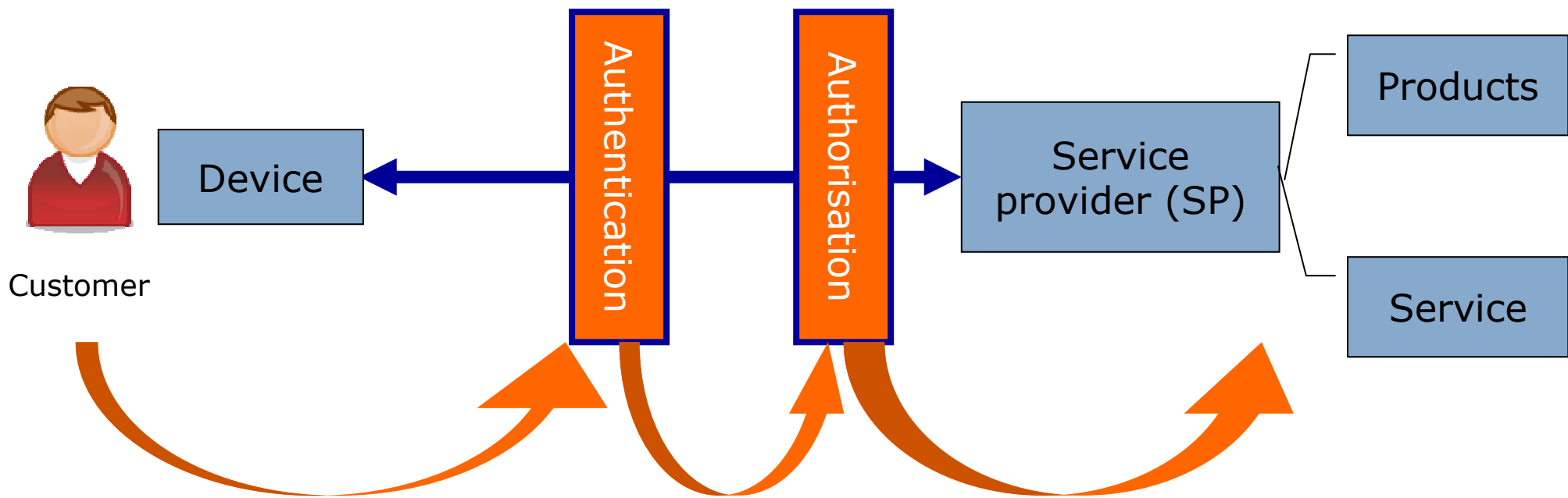
# Service provisioning



Rabobank

Authorisation can only be granted if the identity of the customer is authenticated

To access a service authorisation has to be granted



The customer needs to have his key with him to authenticate himself.

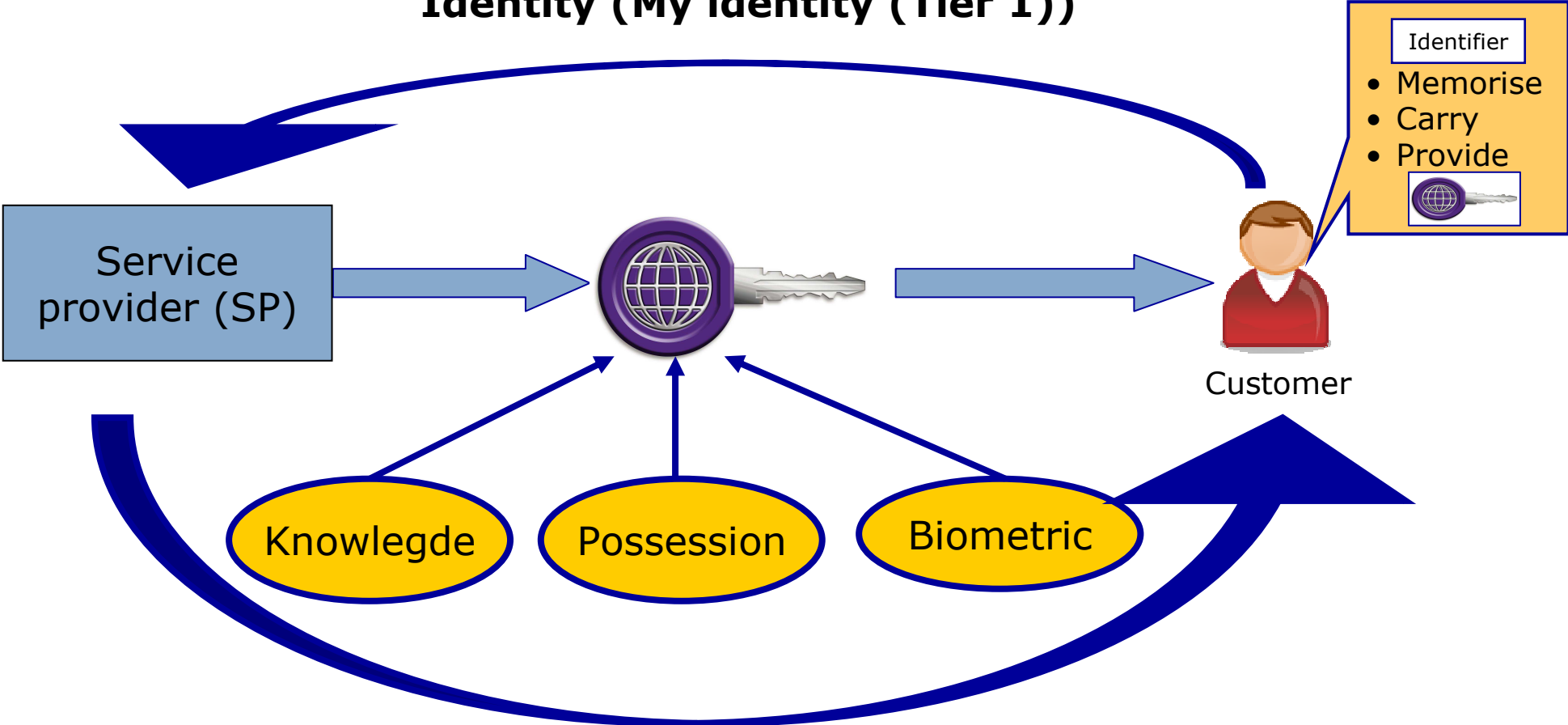


Some kind of provisioning has to be in place for authentication

# Access provisioning



## Identity (My identity (Tier 1))

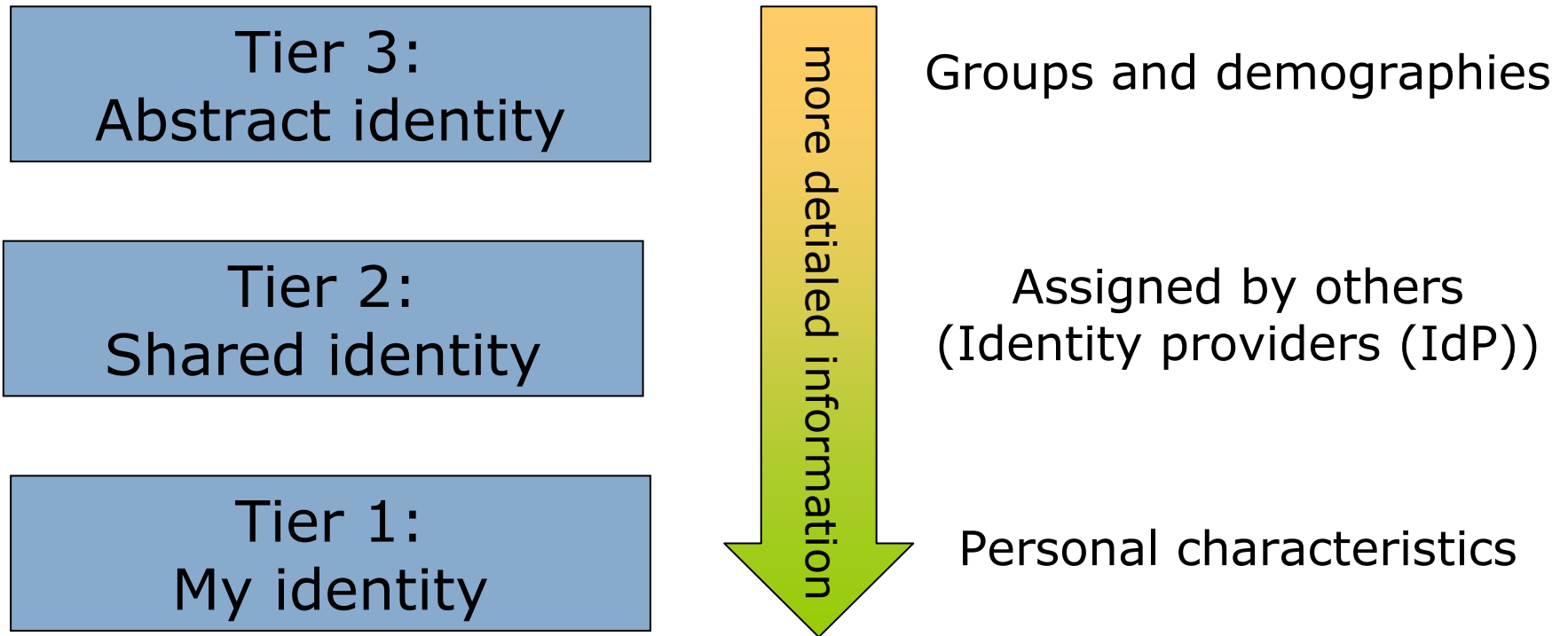


## Identifier (Shared identity (Tier 2))

# Identity perspectives



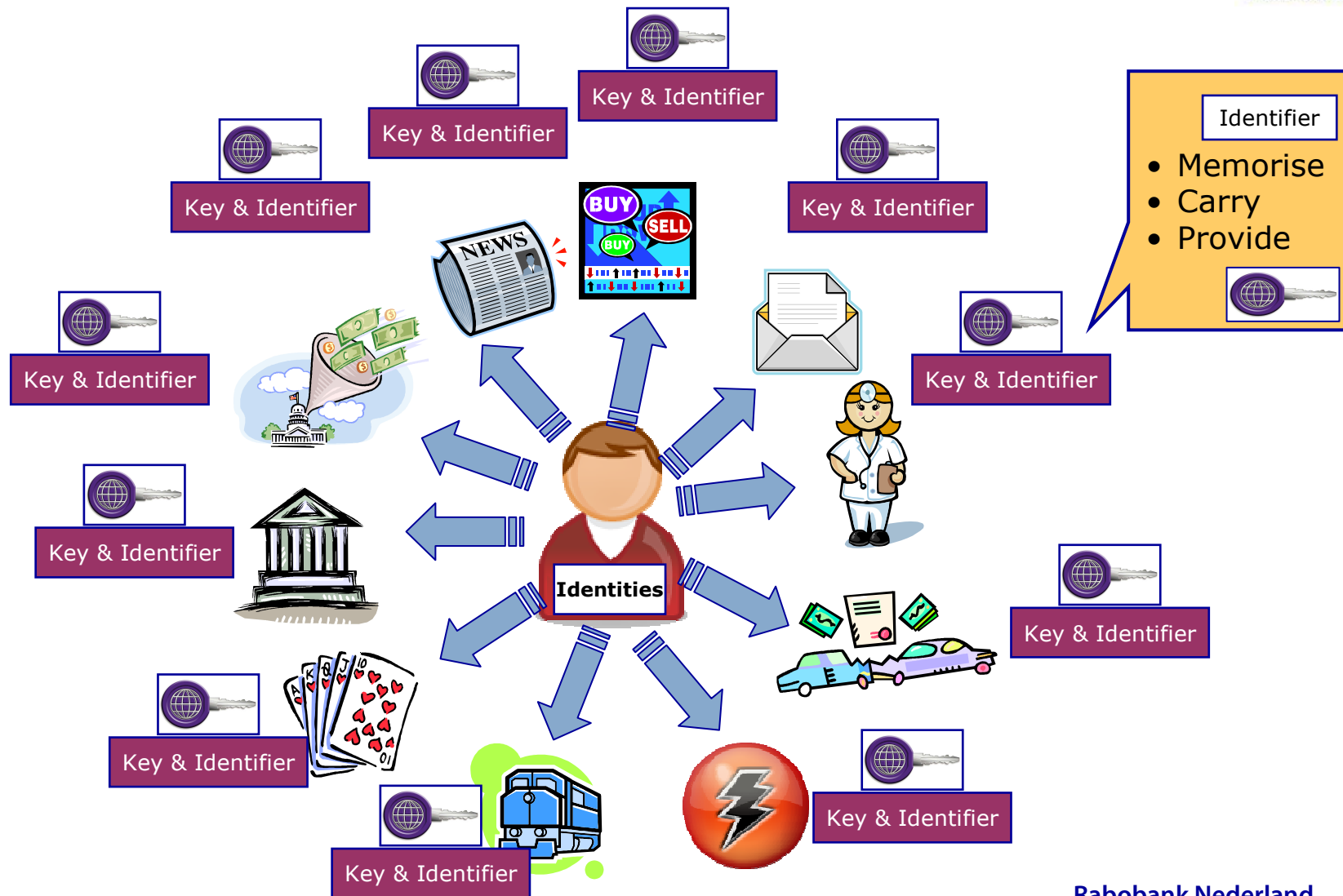
Rabobank





Rabobank

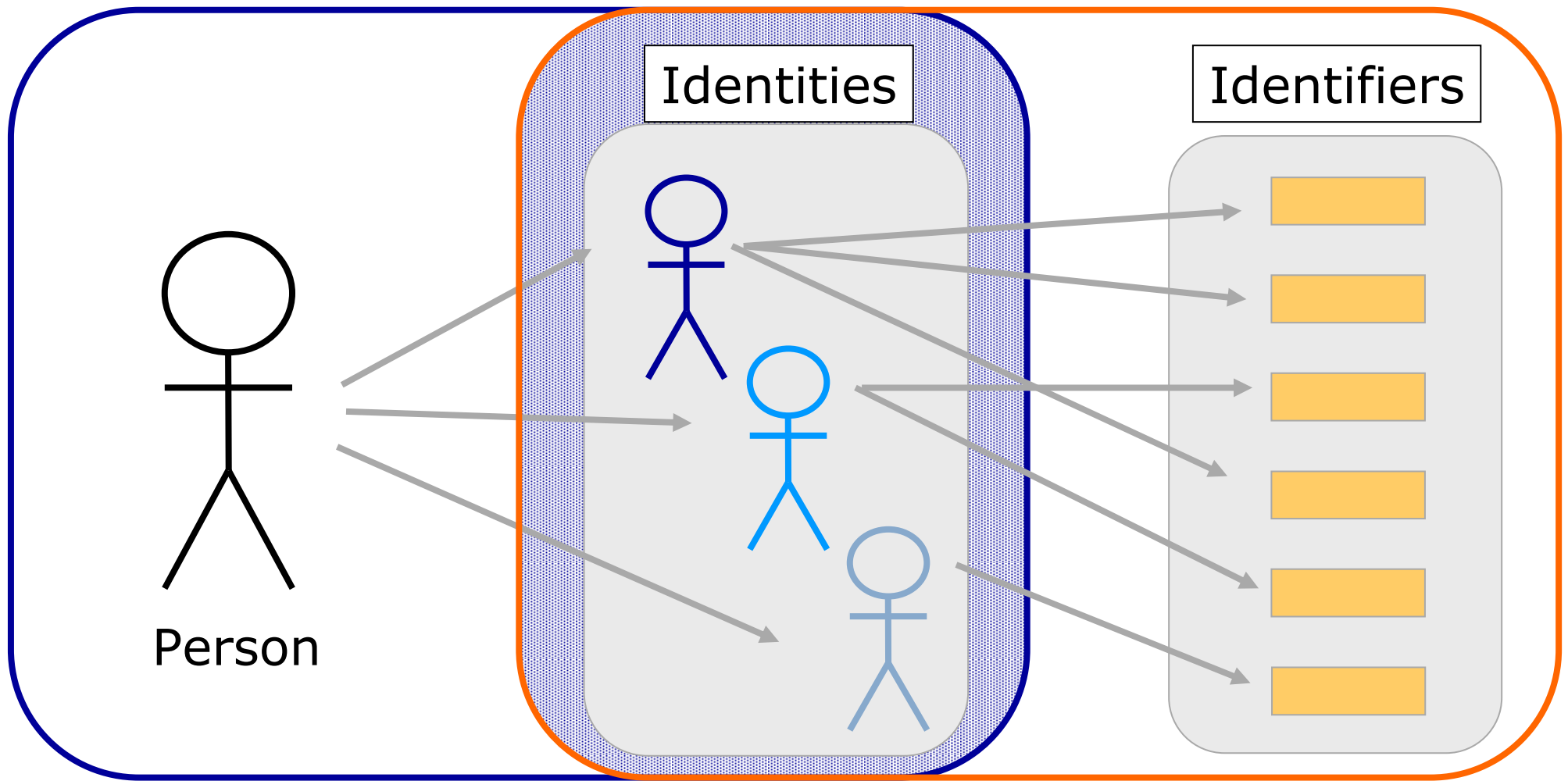
# To access is (not) a problem



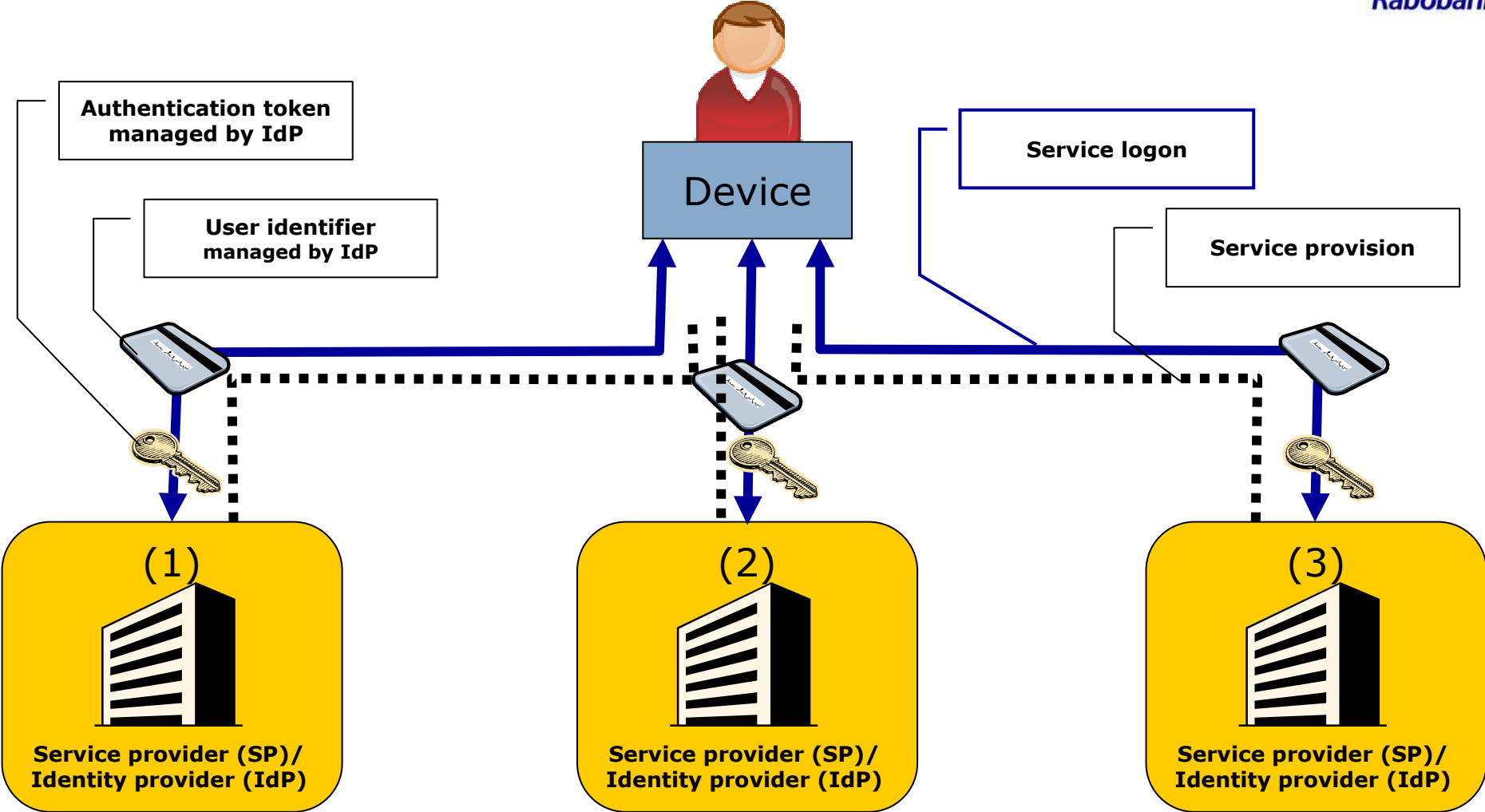
# Identities



Rabobank

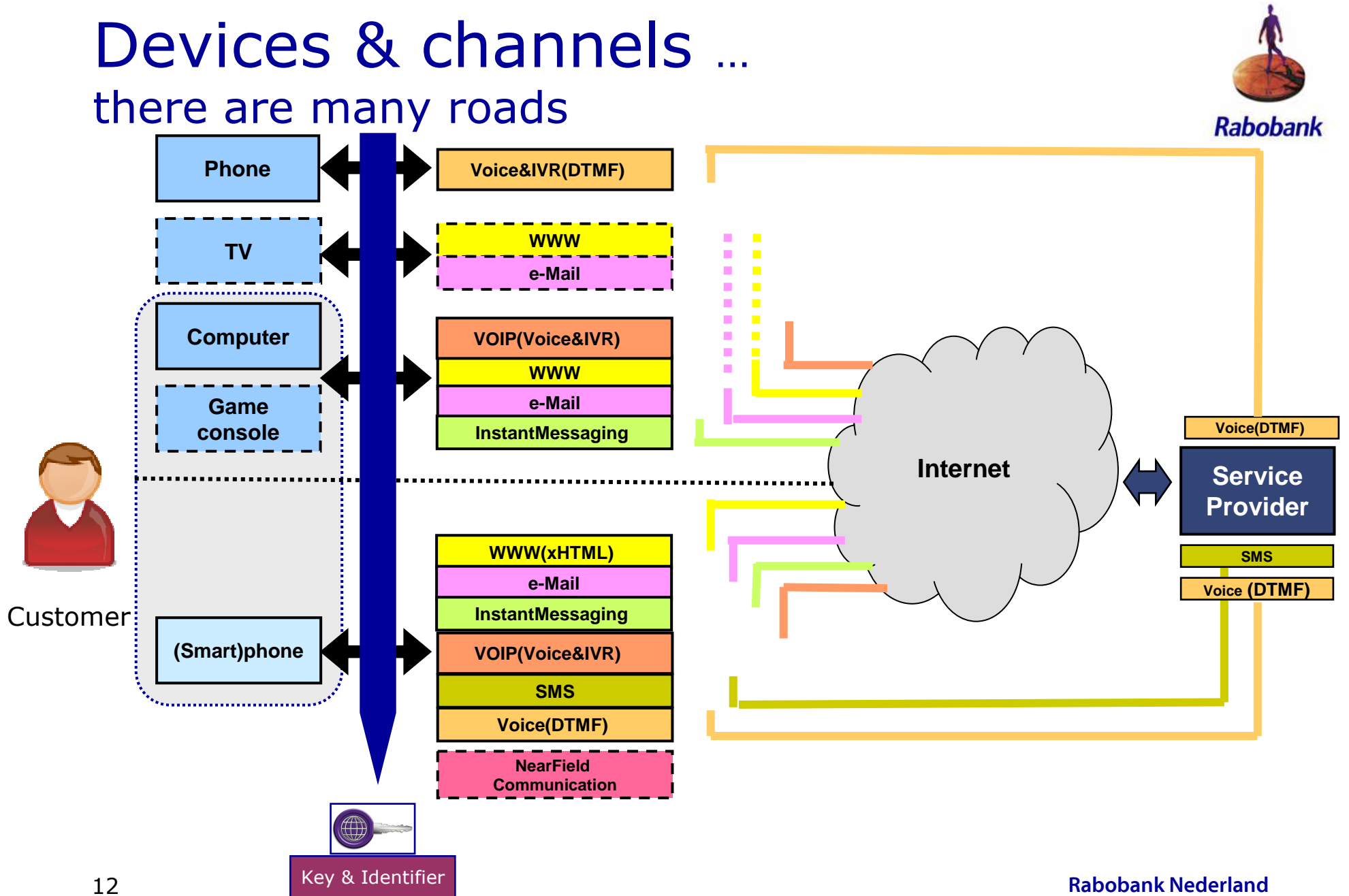


# Silo model

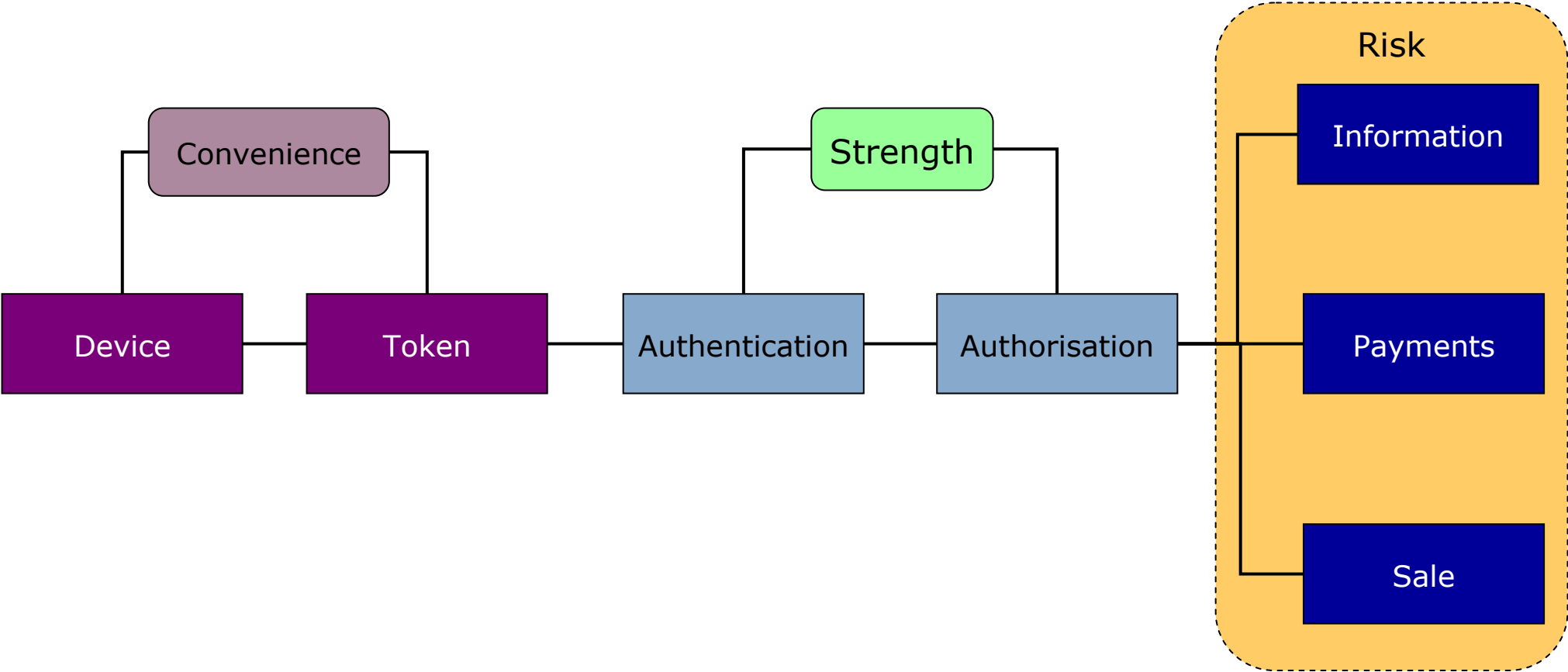


# Devices & channels ...

there are many roads



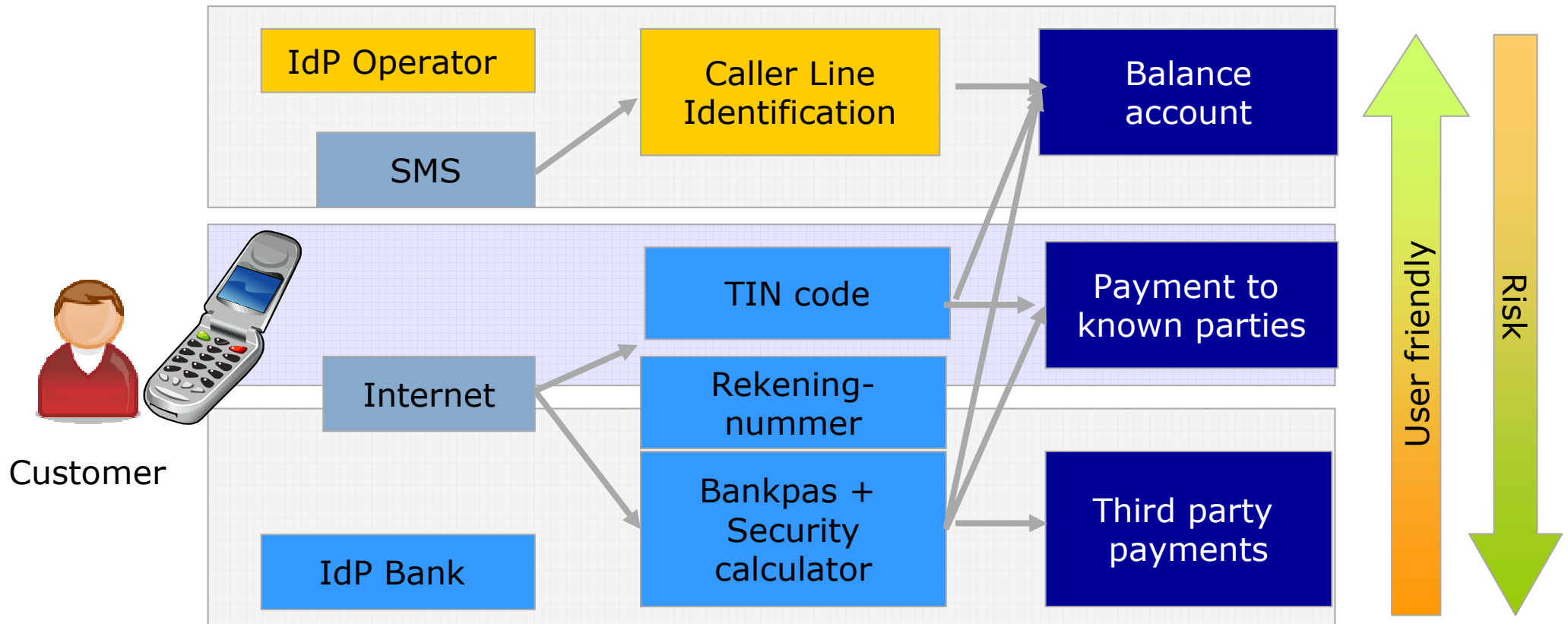
# CSR model



# Multi-channel silo



Rabobank



# Channels, Identifiers, Authentication



Rabobank

Channel		Identitier	Token	Identity Provider	Token provider
Device	Medium				
<b>Telefoon</b>	<ul style="list-style-type: none"> <li>Voice</li> <li>IVR</li> </ul>	<ul style="list-style-type: none"> <li>Name, address, place</li> <li>Klantnummer</li> <li>Caller Line Identification</li> </ul>	<ul style="list-style-type: none"> <li>(TIN code)</li> <li>(TIN code)</li> </ul>	<ul style="list-style-type: none"> <li>Tier 1</li> <li>SP</li> <li>Operator</li> </ul>	<ul style="list-style-type: none"> <li>Customer</li> <li>(Service Provider)</li> <li>(Operator) / (SP)</li> </ul>
<b>Mobile phone</b>	<ul style="list-style-type: none"> <li>Voice</li> <li>IVR</li> <li>SMS</li> <li>E-Mail</li> <li>Instant Messaging</li> <li>Internet</li> <li>NFC</li> </ul>	<ul style="list-style-type: none"> <li>NAW</li> <li>Klantnummer</li> <li>Caller Line Identification</li> <li>Caller Line Identification</li> <li>E-mail adres</li> <li>IM adres</li> <li>Caller Line Identification</li> <li>User naam</li> <li>Klantnummer</li> <li>NFC identity nummer</li> </ul>	<ul style="list-style-type: none"> <li>TIN code</li> <li>(TIN code)</li> <li>(X.509)</li> <li>(Wachtwoord)</li> <li>(TIN) code</li> <li>Wachtwoord</li> <li>Security token</li> </ul>	<ul style="list-style-type: none"> <li>Tier 1</li> <li>SP</li> <li>Operator</li> <li>Operator</li> <li>ISP</li> <li>IM-SP</li> <li>Operator</li> <li>SP</li> <li>SP</li> <li>Fabrikant</li> </ul>	<ul style="list-style-type: none"> <li>Customer</li> <li>Service Provider</li> <li>(Service Provider)</li> <li>(Operator)</li> <li>Certificate Authority</li> <li>IM-Service Provider</li> <li>Service Provider</li> <li>Service Provider</li> <li>Service Provider</li> <li>(Fabrikant)</li> </ul>
<b>PC</b>	<ul style="list-style-type: none"> <li>Stem</li> <li>IVR</li> <li>SMS</li> <li>E-Mail</li> <li>IM</li> <li>Internet</li> </ul>	<ul style="list-style-type: none"> <li>NAW</li> <li>Klantnummer</li> <li>Caller Line Identification</li> <li>Caller Line Identification</li> <li>E-mail adres</li> <li>IM adres</li> <li>Caller Line Identification</li> <li>User naam</li> <li>Customer account number</li> </ul>	<ul style="list-style-type: none"> <li>TIN code</li> <li>(TIN code)</li> <li>(X.509)</li> <li>(Wachtwoord)</li> <li>Wachtwoord</li> <li>Wachtwoord</li> <li>Security token</li> </ul>	<ul style="list-style-type: none"> <li>Tier 1</li> <li>SP</li> <li>Operator</li> <li>Operator</li> <li>ISP</li> <li>IM-SP</li> <li>Operator</li> <li>SP</li> <li>SP</li> </ul>	<ul style="list-style-type: none"> <li>Klant</li> <li>Service Provider</li> <li>(Service Provider)</li> <li>(Operator)</li> <li>Certificate Authority</li> <li>IM-Service Provider</li> <li>Service Provider</li> <li>Service Provider</li> <li>Service Provider</li> </ul>



# Some findings so far



**Rabobank**

- Every service provider issues its own means for authentication
- For authorisation of each service and product we implement a dedicated method of identifying and authentication, based on:
  - It is possible (we have the technology)
  - Convenience
  - Risk
  - Cost
- There is a proliferation of authentication means
  - The customer has to manage them (keep secure)
  - Needs to keep them with him if he wants access
  - Increased risk?
- The use of identifiers issued by other identity providers is rising (e.g. caller line identification)
  - The customer becomes in control (identifier issuer)
  - Has to manage his “identities”
  - Increased risk?
- Service provisioning is (becoming) tightly coupled
  - Devices, channels, possibilities, convenience, opportunities, risk, authorisation

# The road to always access?



Rabobank



- High acceptance
- Convenient
- Multi-purpose
- (almost) always with me
- Can be used (mostly) any time, any place, anywhere ...
- Identifier always available

# Concept IBM (Android)



Rabobank

## Information Card



Example shows cell phone based on open, Linux-based software platform

### Software and device

- Open software platform (Mobile Open Linux)
- Supports various hardware platforms (PC, PDA, Cell Phone, ...) and delivery methods

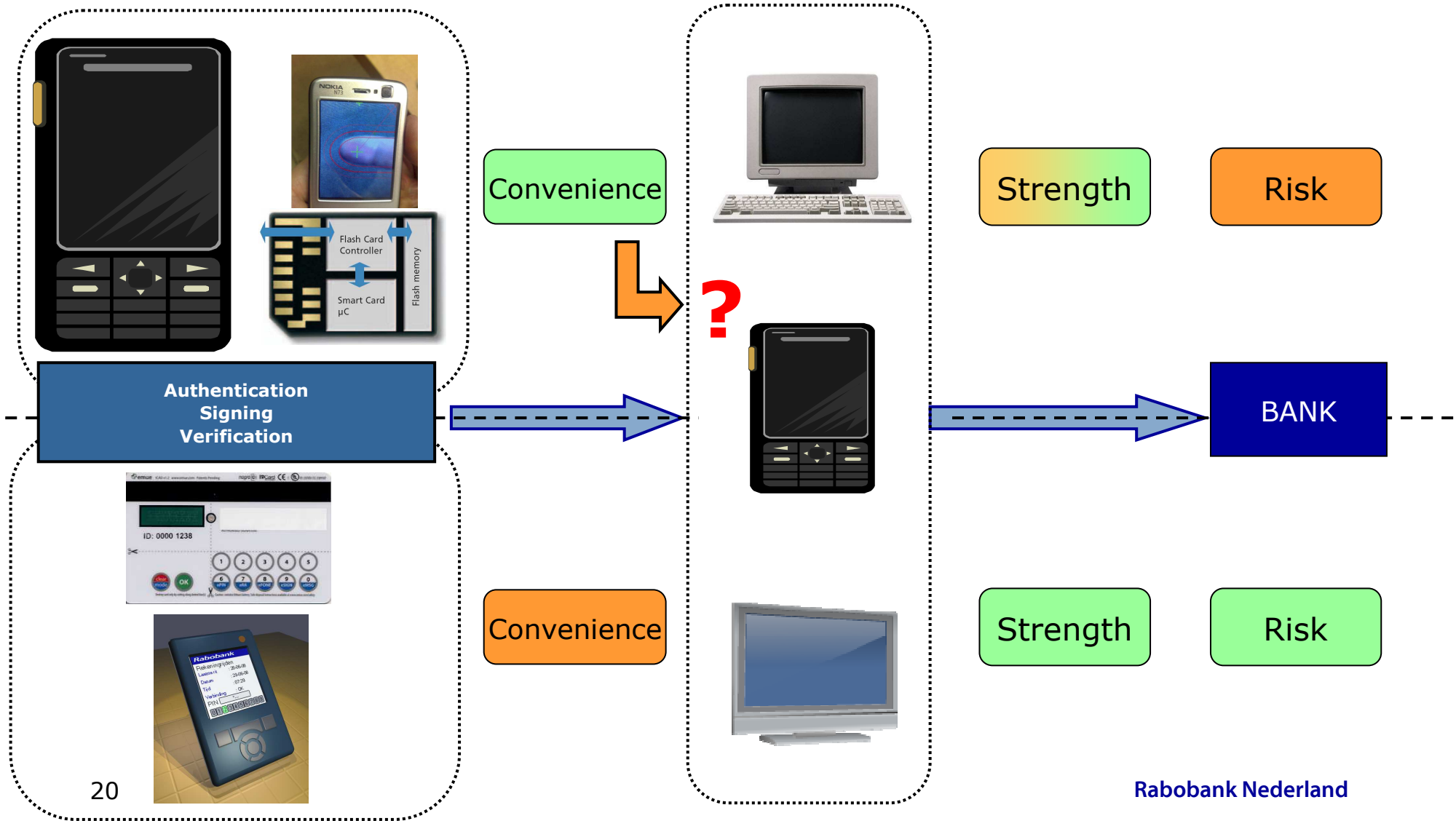
### Information Card

- Inspired by physical id cards
- Representation of a specific set of identity attributes
- Users might have several cards, from several issuers
- Client offers support for managing and selecting cards, and attributes from a card

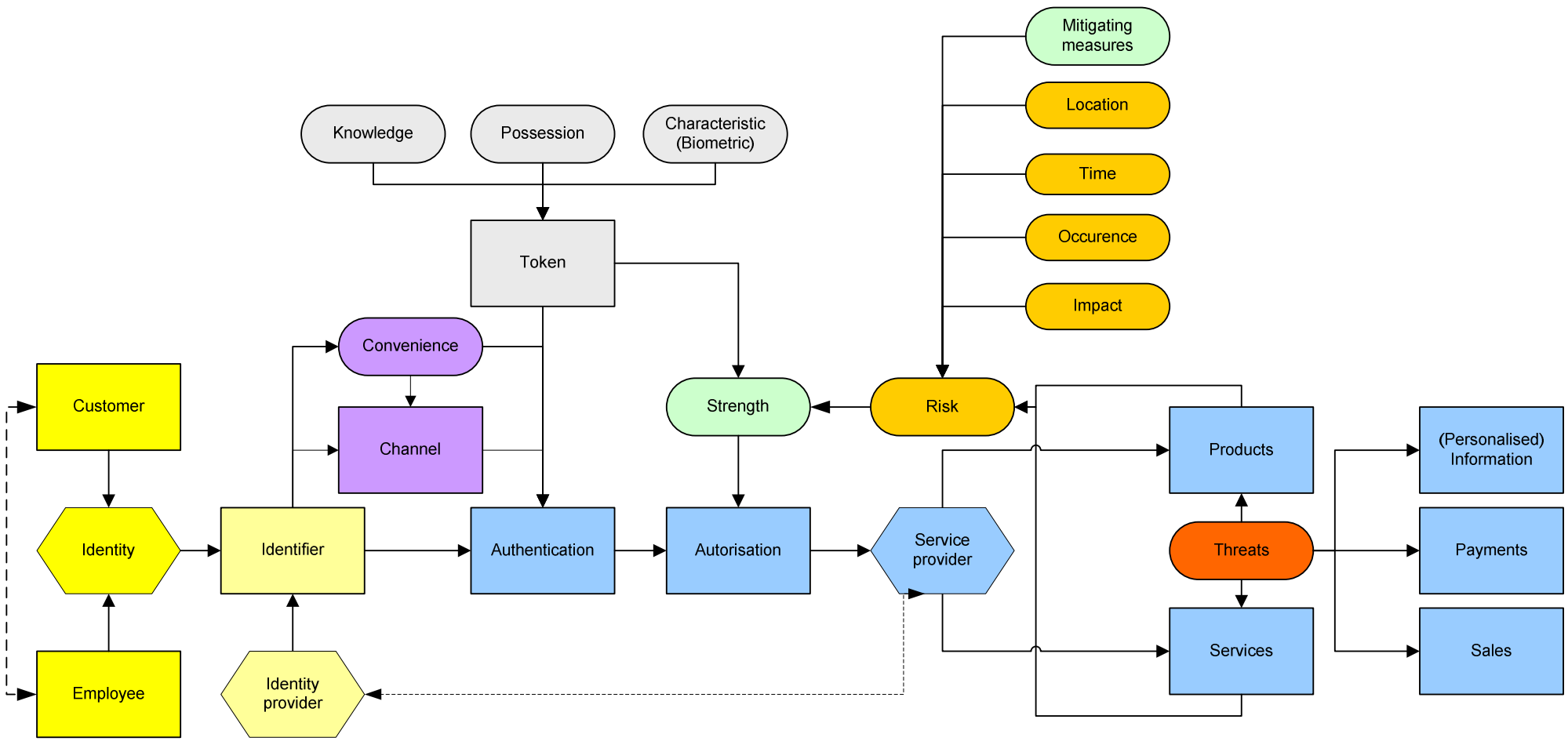
### Cryptographic Protocols

- Obtain, select, show card, etc. are translated into cryptographic tokens and message flows
- Actual data might be
  - Local and static, on the device
  - Remote, with the IP, and possibly dynamic
- Details are hidden from the user

# The key(s) to always access: some challenges



# The CSR model (so far)





*Rabobank*

Questions ?