PrimeLife

Reference Group Meeting

March 23 – 24, 2009

Session 1: PrimeLife Usability Work

A research project funded by the European Commission's 7th Framework Programme

Session 1: Usability

- Background
- **Simplified *privacy preferences* management**
- **Anonymous *credential selection* user interfaces**
- ***Trust evaluation* user interfaces**

Discussion and Feedback

Privacy-enhanced Interactions – Technology

1 Simplified privacy preferences managemen

Non-intrusive, intuitive definition of user preferences

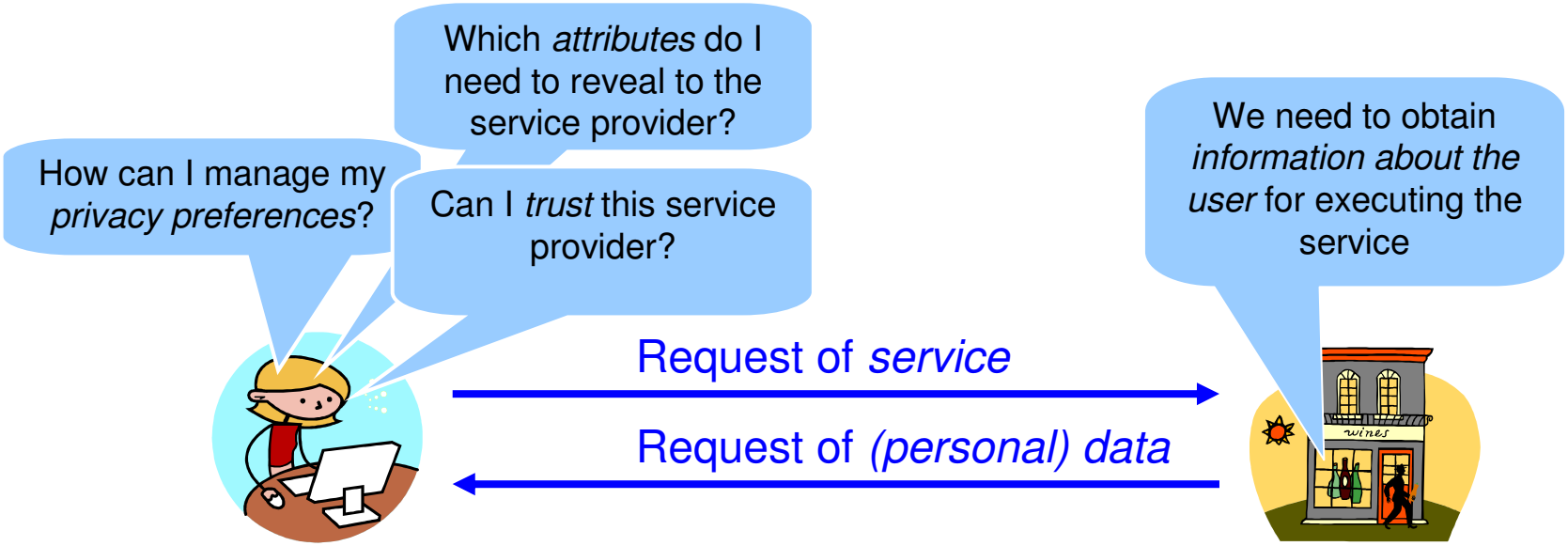
2 Anonymous credential selection

Decision on attribute information to be revealed

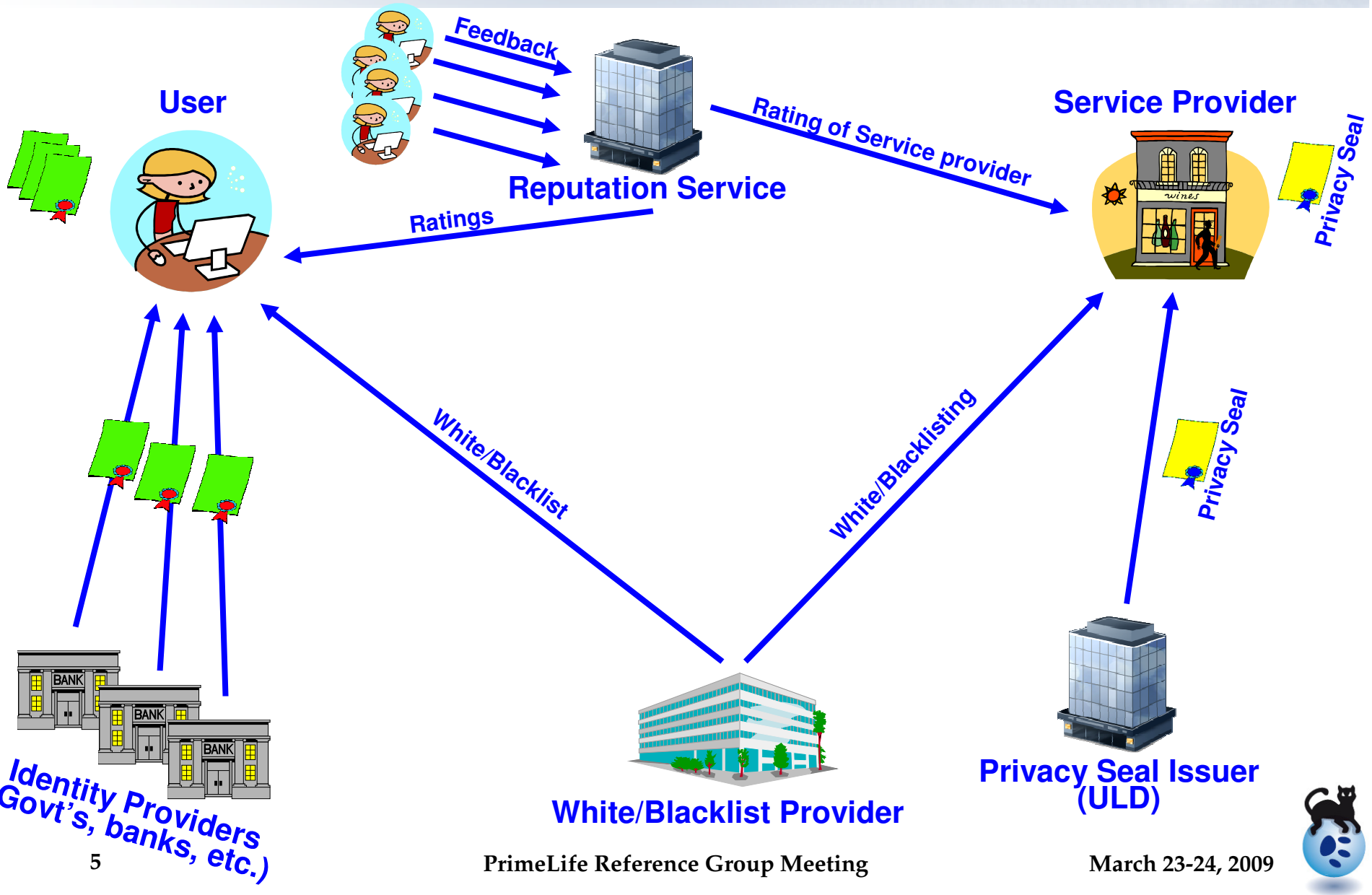
3 Trust evaluation

How users can establish trust in service providers

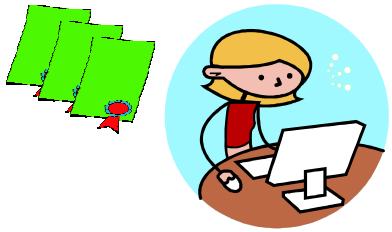
The Setting


Which *attributes* do I need to reveal to the service provider?
How can I manage my *privacy preferences*?
Can I *trust* this service provider?
We need to obtain *information about the user* for executing the service
Request of *service*
Request of *(personal) data*
wines

The Architecture



An Interaction



White/Blacklist query

Ok

Request of **service**

Privacy Seal

Data request; data handling proposal
- A valid service subscription and its type
- Proof of age > 14 years

Evaluation of request

Request of **trust & assurance data and evidence**

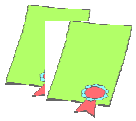
We can offer the following:
- A privacy seal issued by ULD
- We are running a PrimeLife-enabled system including a privacy policy negotiation management engine
- …

Trust assessment against local trust & assurance policy

Trust → Trust & assurance evaluation

Preferences → Display of privacy policy
Privacy preferences management

Credentials → Display of data request
Identity selection



Subscription.type = “Basic”
Date of birth < “1995-03-23”
Proof = <*Binary blob*>

Negotiation

Session 1: Usability

- Background ✓
- **Simplified privacy preferences management**
- **Anonymous credential selection user interfaces**
- **Trust evaluation user interfaces**

How to simplify Privacy Preference Management?

- Assumption: Users will not do complex privacy preference settings beforehand
- Our approach:
  - Provide a predefined privacy preferences that can be adapted ”on the fly” according to the user’s behaviour
  - Take the most privacy-friendly preference as a default

Privacy Preference Types (”PrivPrefs”)

- 3 predefined PrivPref-Types:
  - Anonymous
  - Only Minimal Data
  - Additional Data
- PrivPref-Structure:

  (”Anonymous”| ”Only Minimal Data”, contact, purpose)

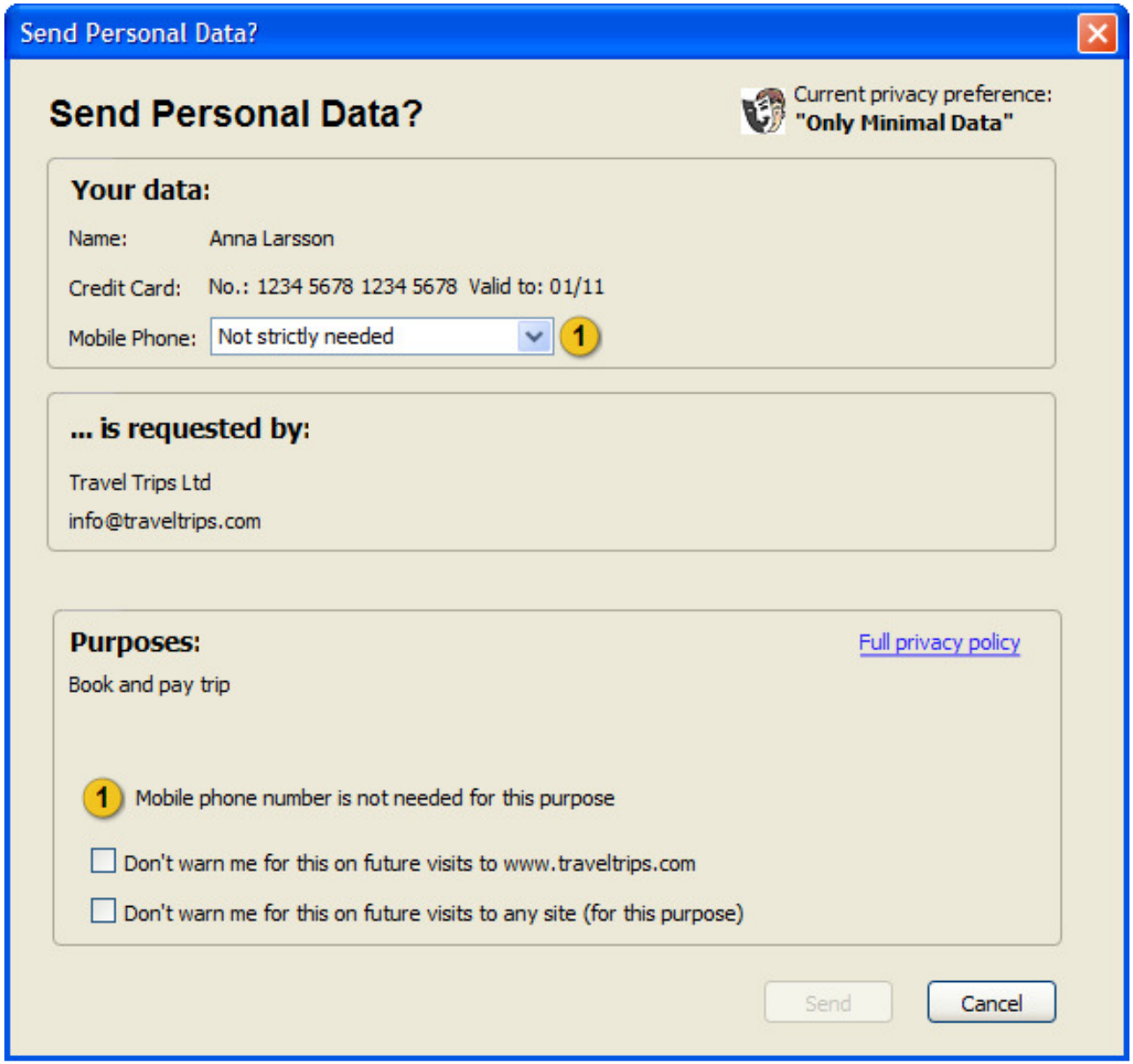
  or

  (”Additional Data”, contact, purpose, data categories)
- In addition, we need a table of necessary data categories for purposes, i.e. with entries (purpose, data categories)

PrivPref-Management ”on the fly”

- If a user contacts a side (contact) for a specific purpose:
  - Check whether there exist a PrivPref for (contact, purpose)
  - If yes: Use this PrivPref
  - If no: Use PrivPref (”Anonymous”, contact, purpose)
    (or (”Only Minimal Data”, contact, purpose))
- If ”more data” is requested than allowed by current PrivPref: Inform the user and provide the possibility to adapt/change PrivPref settings ”on the fly”.

Example: Current PrivPref "Only Minimal Data"



HCI for Anonymous Credential Selection

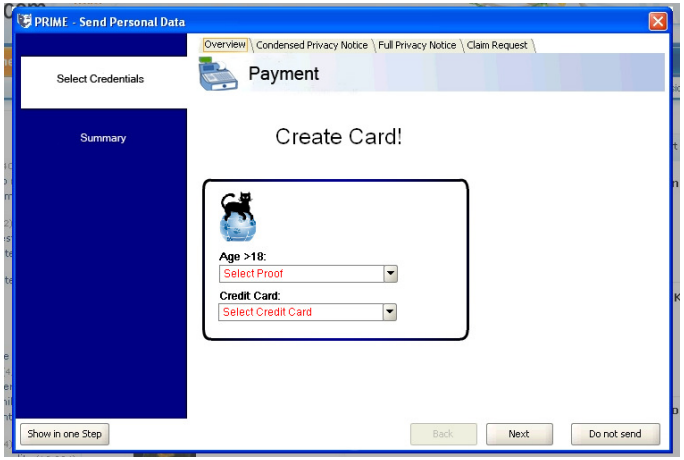
- Problem: No obvious real-world analogies exist - Difference to real-world credentials:
  - Only parts of the credential attributes or characteristics of attributes can be proven/revealed
  - Different credential shows are unlinkable
- What mental models can be developed or can be accounted on?

Test task: buy something

Paying [In General]

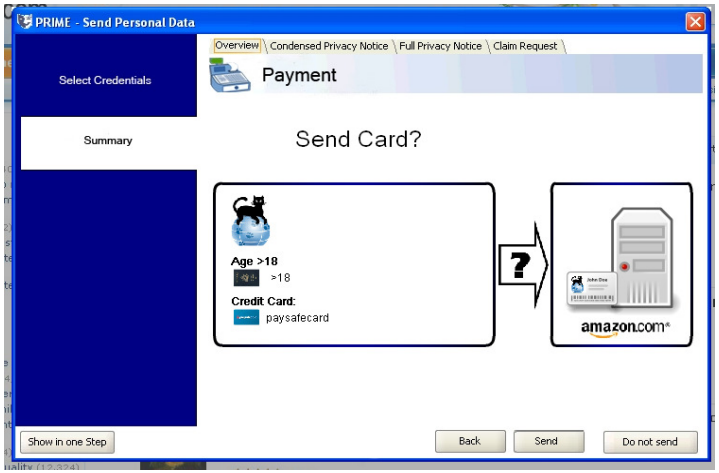
1

Assemble Data



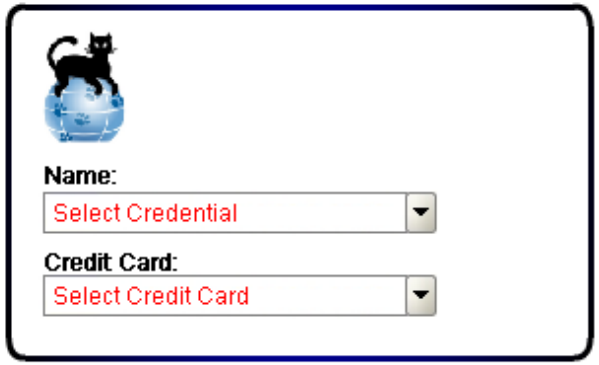
2

Send Data

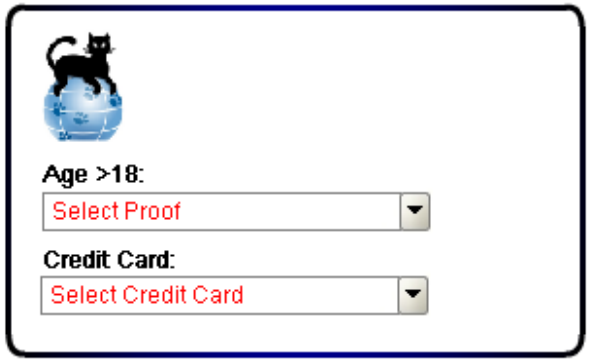


1st Iteration of Mockups - Paying [Scenarios]

Selecting Parts of Credentials

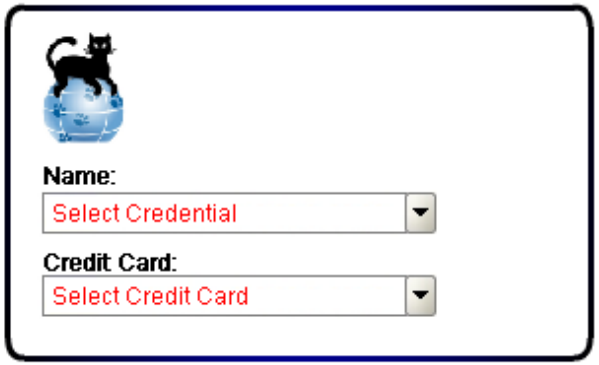


Proofs of Characteristics with Credentials

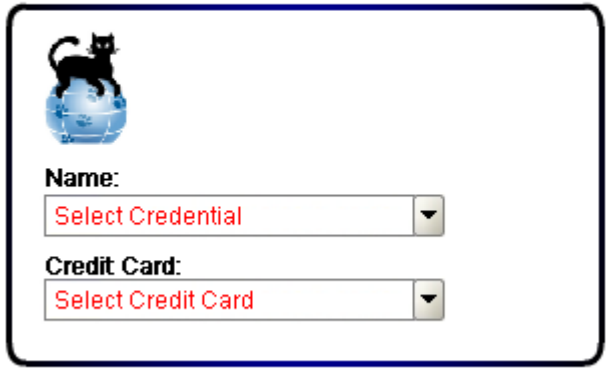


Assembly [Mental Models]

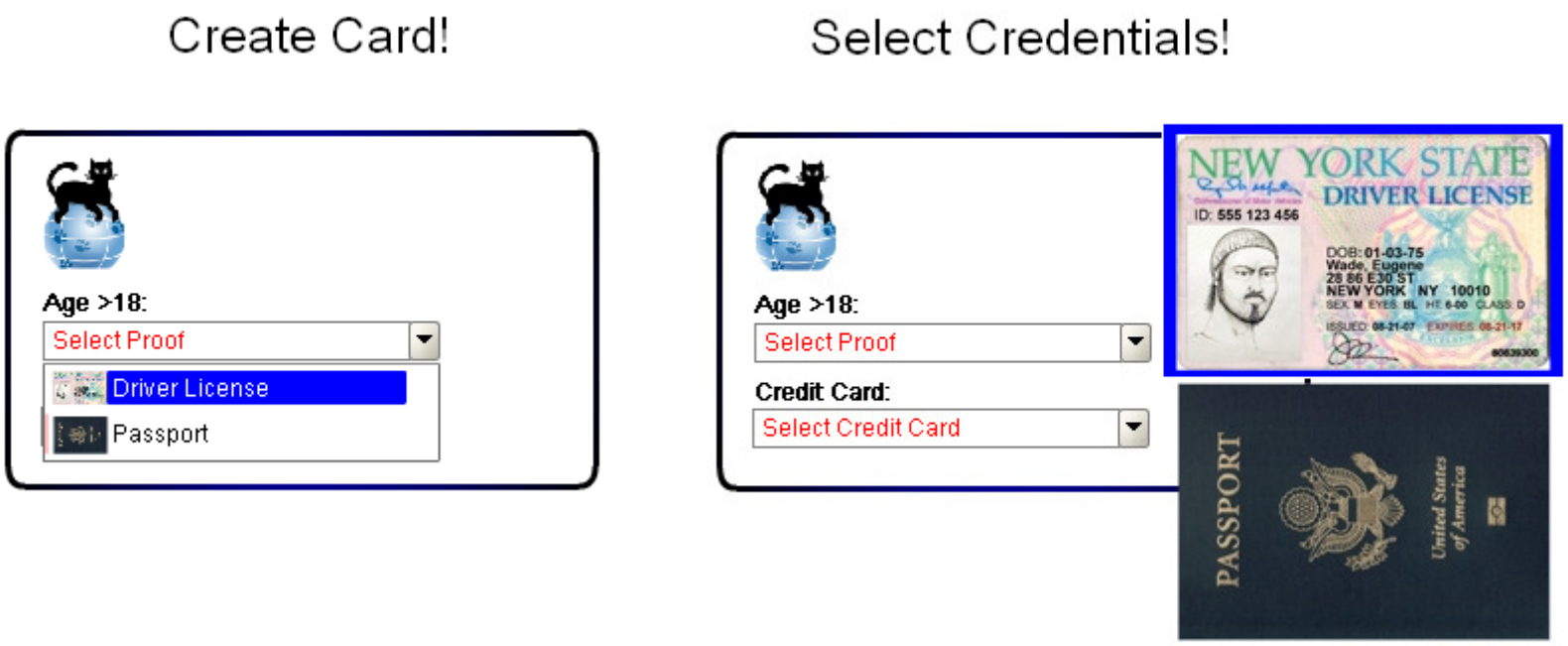
Create Card!



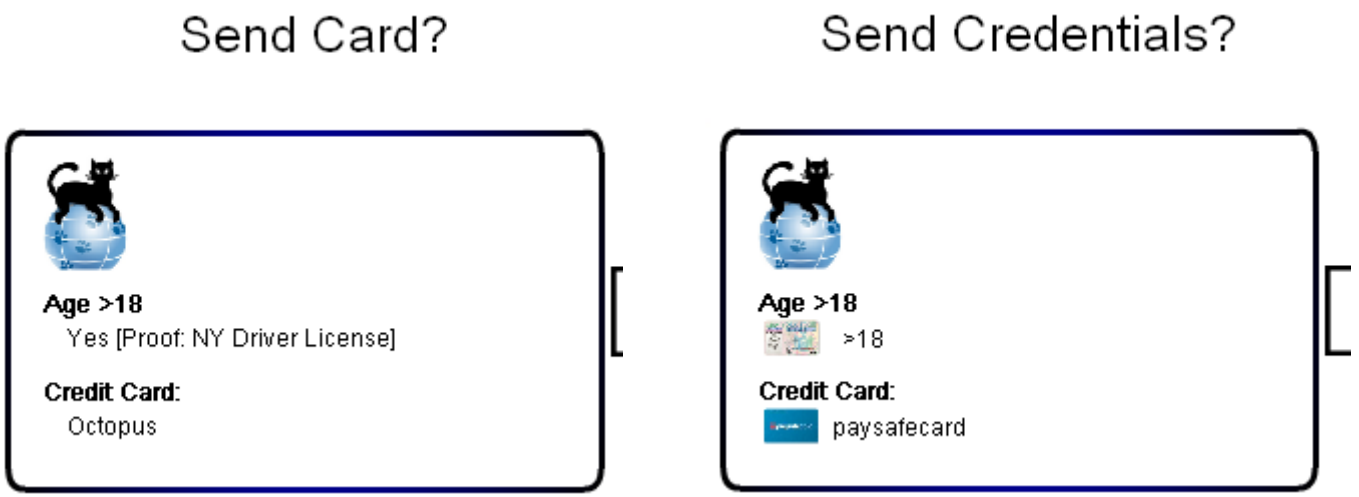
Select Credentials!



Assembly [Selection Mechanism]



Send data [Text/Icons]



Questions [Data sent?]

What does Amazon.com know about you? Tick the boxes and fill in the blanks below if you need to!

Questions [Data sent?]

	Förnamn
	Efternamn
	Födelsedagj
	Förarbehörighet
	Utfärdandedatum
	Utgångsdatum

Övrigt: _____

Övrigt: _____

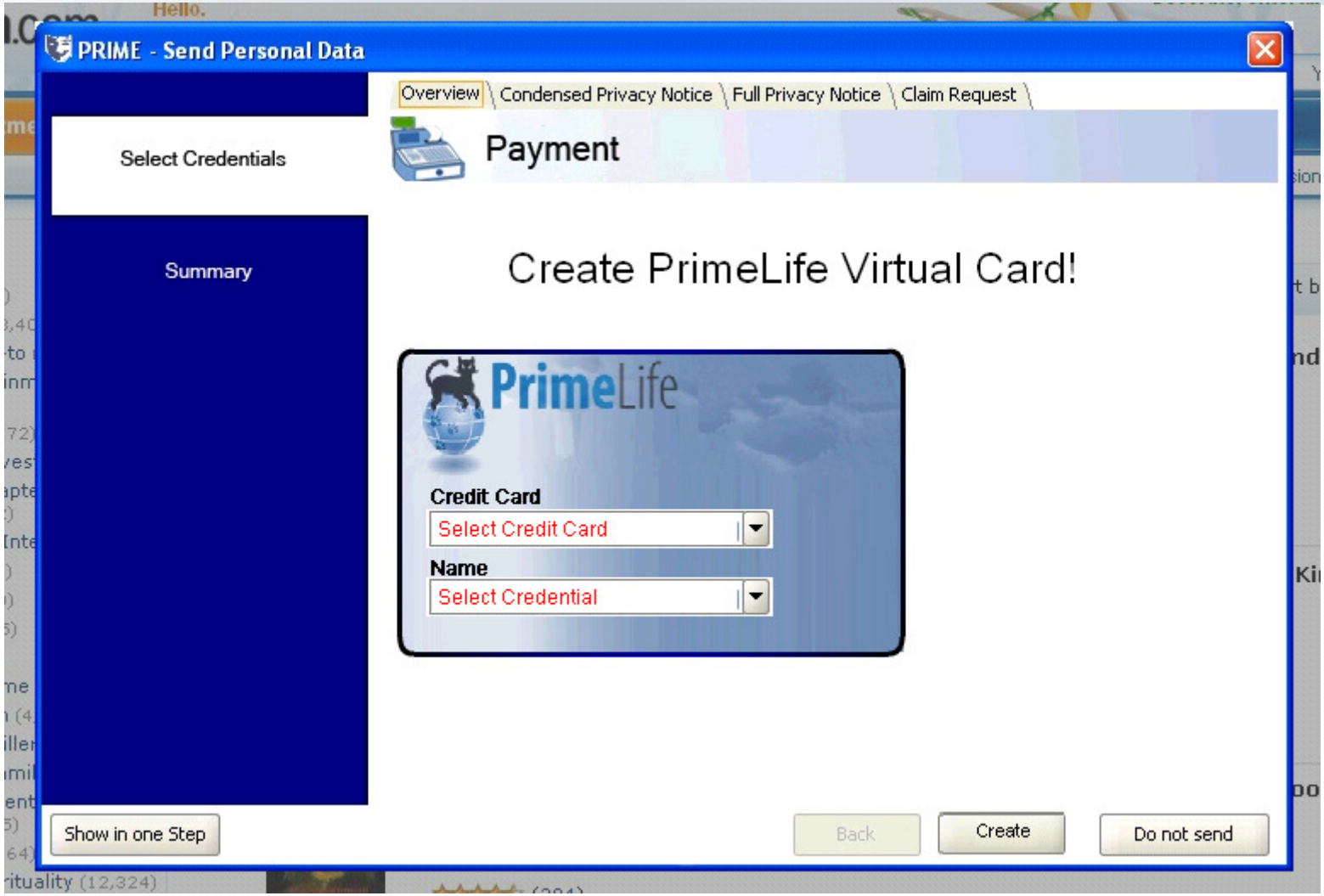
Test results – 1st Iteration

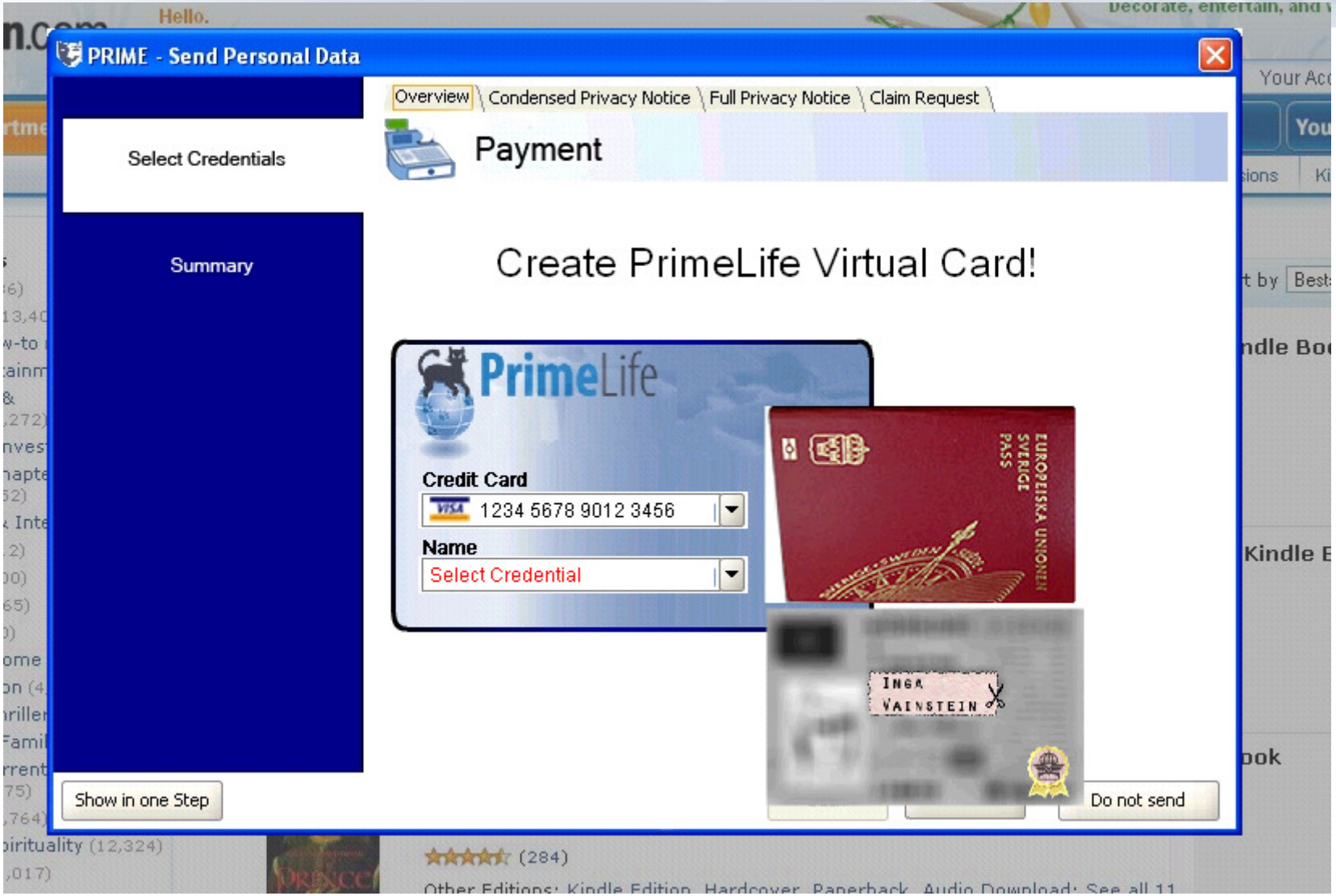
40 participants

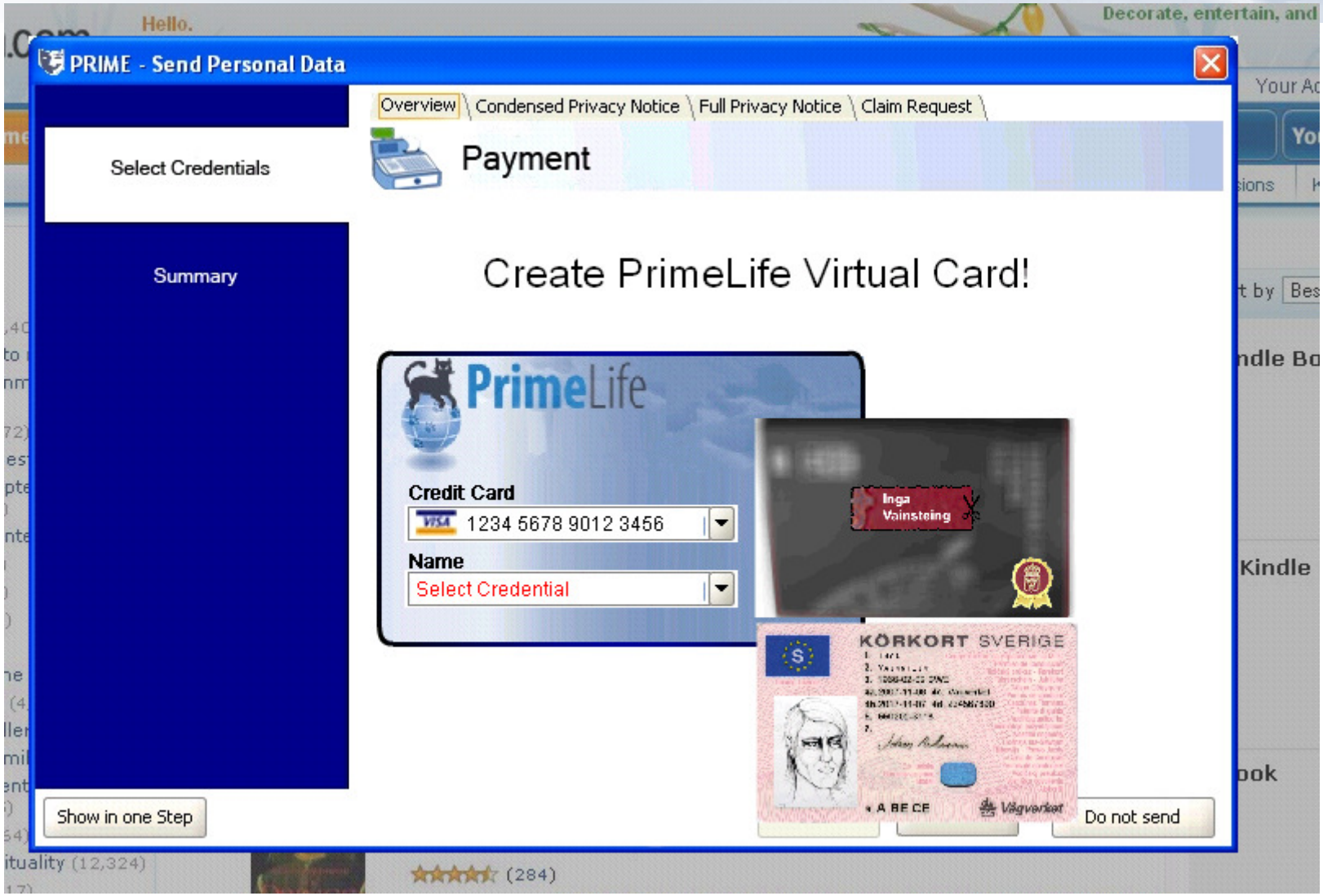
3 got it!

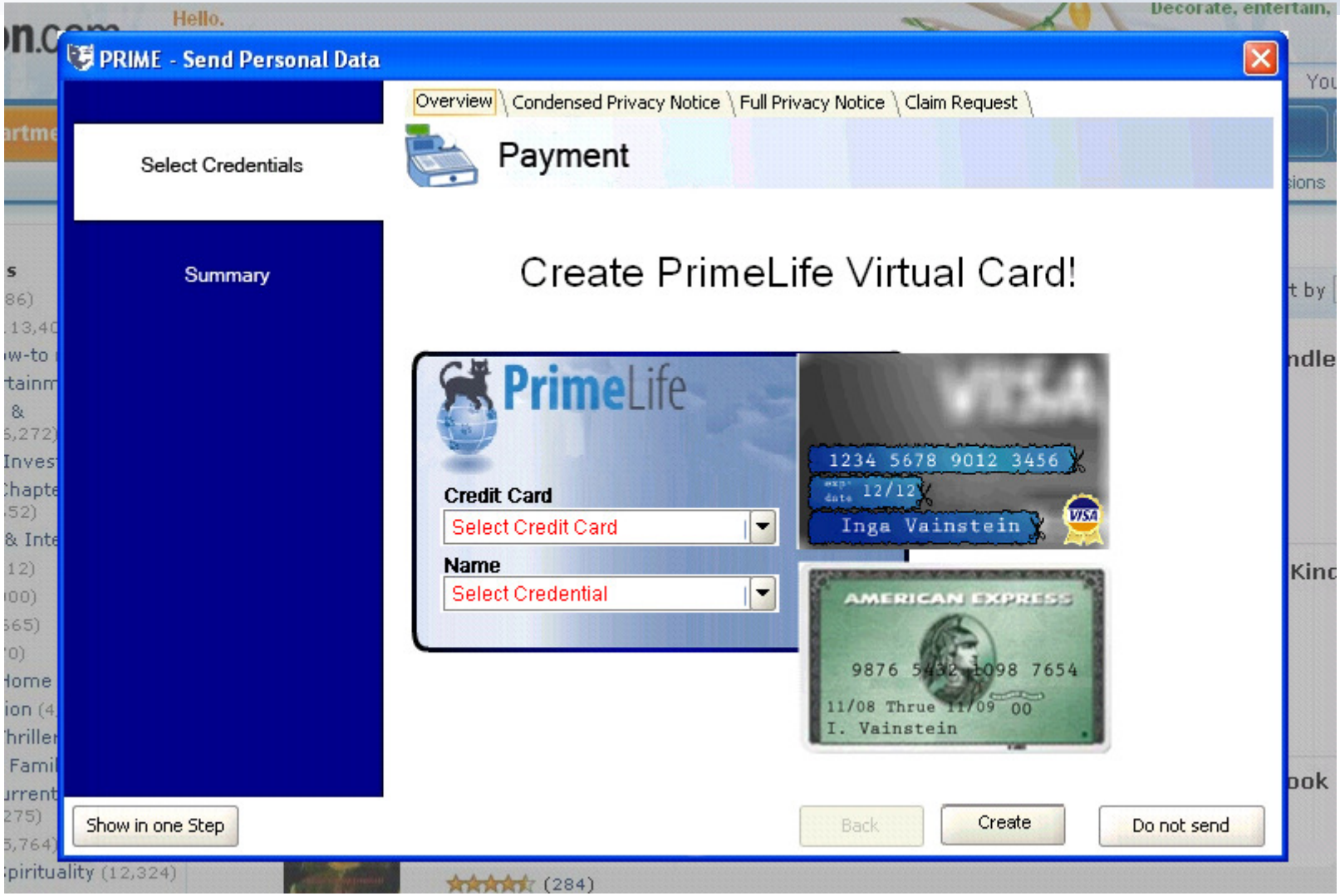
(7,5%)

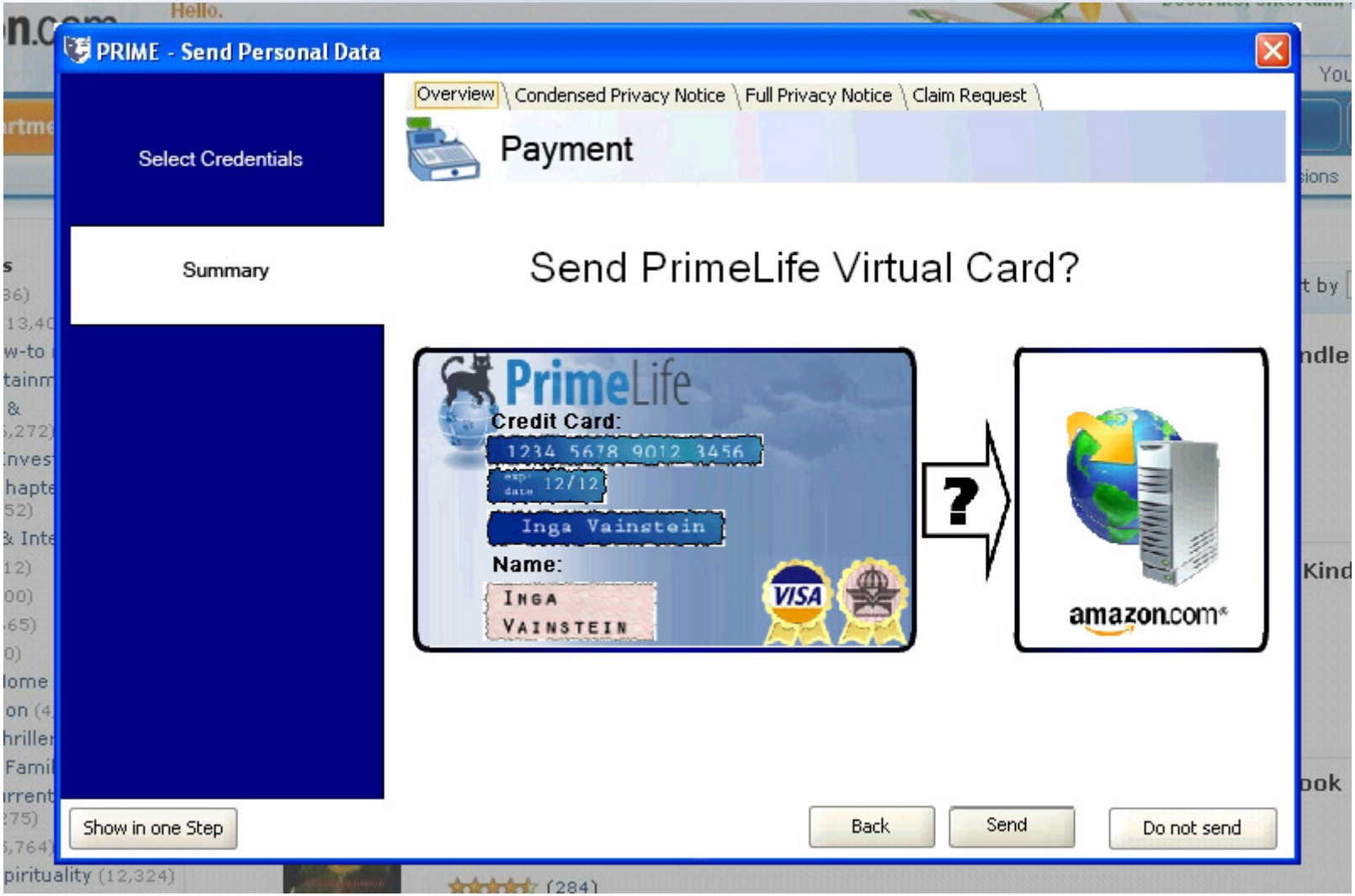
3rd Iteration of Mockups




PRIME - Send Personal Data
Overview
Condensed Privacy Notice
Full Privacy Notice
Claim Request
Select Credentials
Summary
Payment
Create PrimeLife Virtual Card!
PrimeLife
Credit Card
1234 5678 9012 3456
Name
Select Credential
Show in one Step
Do not send


PRIME - Send Personal Data
Overview
Condensed Privacy Notice
Full Privacy Notice
Claim Request
Select Credentials
Summary
Payment
Create PrimeLife Virtual Card!
PrimeLife
Credit Card
1234 5678 9012 3456
Name
Select Credential
Inga Vainsteing
KÖRKORT SVERIGE
Show in one Step
Do not send


PRIME - Send Personal Data
Overview
Condensed Privacy Notice
Full Privacy Notice
Claim Request
Select Credentials
Summary
Payment
Create PrimeLife Virtual Card!
PrimeLife
Credit Card
Select Credit Card
Name
Select Credential
1234 5678 9012 3456
12/12
Inga Vainstein
AMERICAN EXPRESS
9876 5432 1098 7654
11/08 Thrue 11/09 00
I. Vainstein
Show in one Step
Back
Create
Do not send


PRIME - Send Personal Data
Select Credentials
Summary
Overview
Condensed Privacy Notice
Full Privacy Notice
Claim Request
Payment
Send PrimeLife Virtual Card?
PrimeLife
Credit Card:
1234 5678 9012 3456
exp date 12/12
Inga Vainstein
Name:
INGA VAINSTEIN
VISA
?
amazon.com
Show in one Step
Back
Send
Do not send

Result – 3rd Iteration

5 participants

2 got it!

Next Steps?

- Error of measurement?
- Show MouseOver state or only cut-outs?
- Scrap the card metaphor?

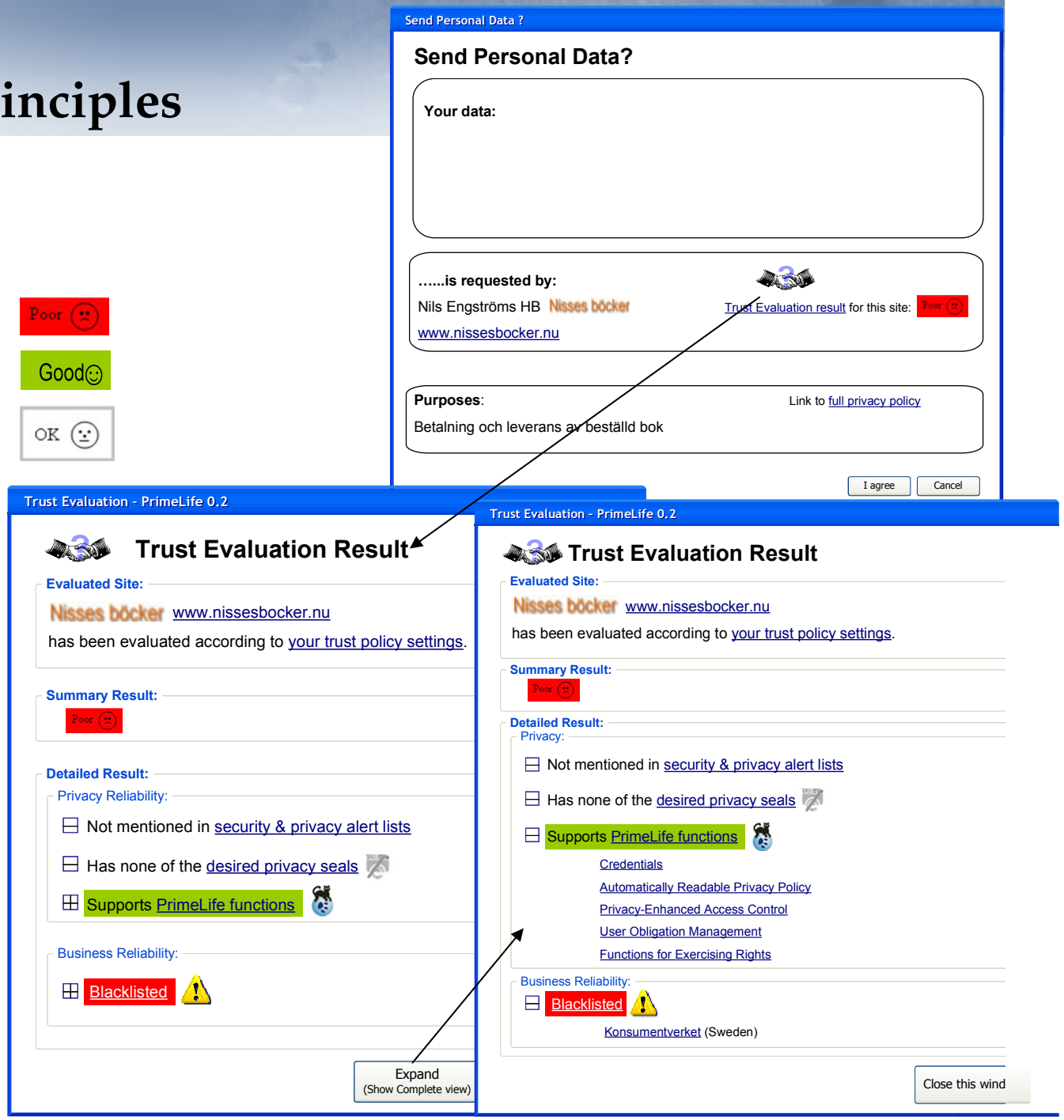
- Suggestions from the Primelife General Meeting:
  - Black out lines
  - Drag and drop or Animations
  - Send partial cards / send selected pieces
  - Select verifiers instead of cards
  - Combining with tutorial
  - Add text:
    - “Please note that this data is not sent”
    - “Please note that only this data is sent”

HCI for Trust evaluation of Services Sides – *Challenges:*

- Find suitable trust & assurance parameters
  - *Has Privacy seals*
  - *Mentioned on security & privacy alert lists*
  - *Blacklisted*
  - *Supports PrimeLife functions*
  - *(To be included next: reputation ratings)*
- Illustrate parameters with different semantics & scopes
- Find intuitive icons
- Address usability problems
  - *Users have difficulties to differentiate between user and services sides*
  - *Extensive warnings can be misleading*

Our Design Principles

- Use multilayered structure
- Use a selection of meaningful overall evaluation results
- Make clear who is evaluated
- Use several UI concepts for informing the users
- Group evaluation results into sub categories ”*Privacy*” and ”*Business Reliability*”



Test results of two mockup iterations (I)

Positive results +:

- Good understanding of the “Send Personal Data?” user interfaces and presented top-level trust evaluation results
- The “Good” and “Poor” emoticons on top level were also clearly understood by all users.
- All participants also clearly understood that the services side and not the user side was evaluated
- The colours red and green in the prototype (both on icons and over text) were all understood correctly by the participants.
- The icon for alarming the users was also correctly understood.
- Majority of participants like the function they tested to be called “Trust Evaluation”.
- All participants said in the interviews that they would like to use a PrimeLife prototype including a Trust Evaluation function that is similar to the one that was tested.

Test results (II)

Issues -:

- More detailed trust evaluation results on the second layer, both red and green colours, were harder to understand
- Some icons used in the 1st mockup version were hard to understand:



or made them suspicious:

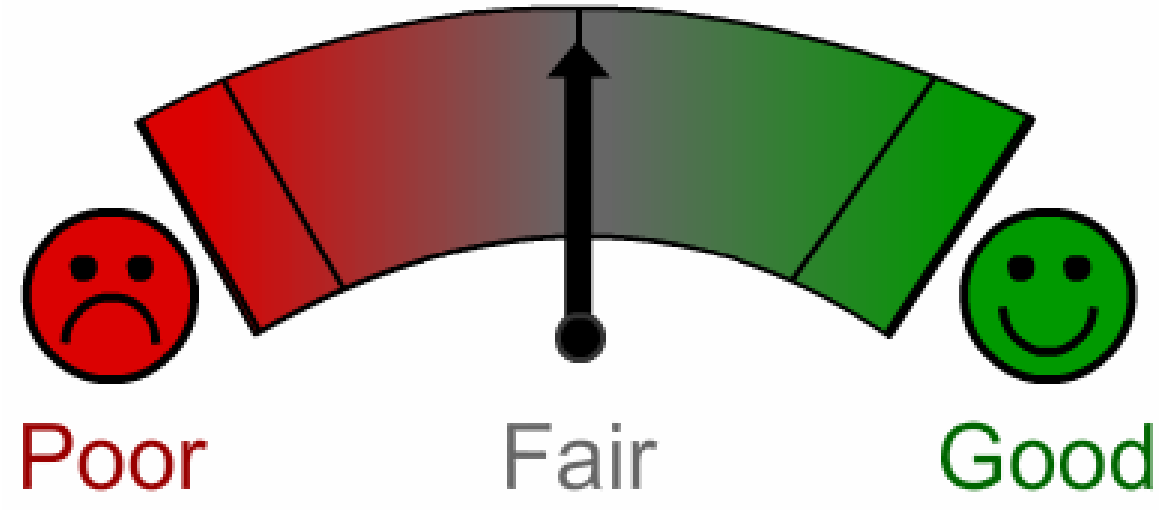

…. and were replaced:

- "Neutral" evaluation result ("Not bad", "ok", "No alarm") hard to understand for some participants.
  New suggestion: "Fair"

- Confusion on how trust evaluation can work if PrimeLife is not enabled.

To be tested next…..

Trust meter for illustrating overall results:



Discussion and Feedback