UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Information flow control for static enforcement of user-defined privacy policies

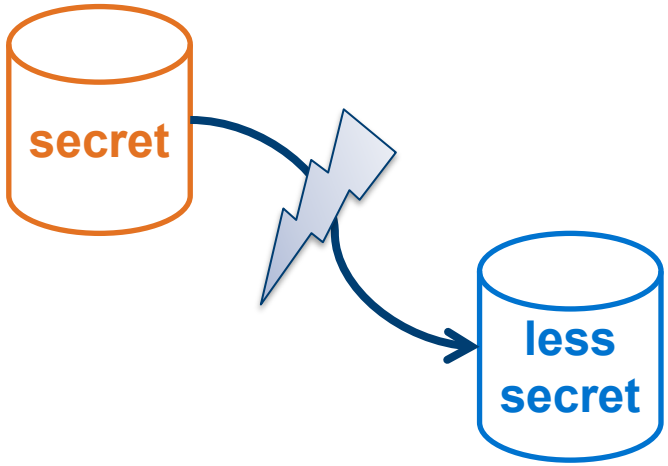
Sören Preibusch

POLICY 2011

7th June 2011

Credible privacy guarantees beyond collection

- **IFC: Keep information flows separate, by policy**
- **Explicit information flow**
  - Assignment
  - I/O
- **Implicit information flow**
  - Control flow, conditional exec.
  - Timing
  - Exceptions, termination




```
less_secret = secret;
newsletter_addr += "," + email;
```

JIF: Java + information flow

- **Java type + JIF label**
  - String{pCustomer->pMarketingDept} sEmail = "sdp36@cl";
- **JIF ecosystem**
  - jifc: compiles, intermediate code, static analysis (expl. + impl.)
  - jif: shorthand for java + runtime classes
  - Runtime classes: dynamic analysis
  - Library classes: dynamic label creation and manipulation

Labels and principals: creation, application, ordering

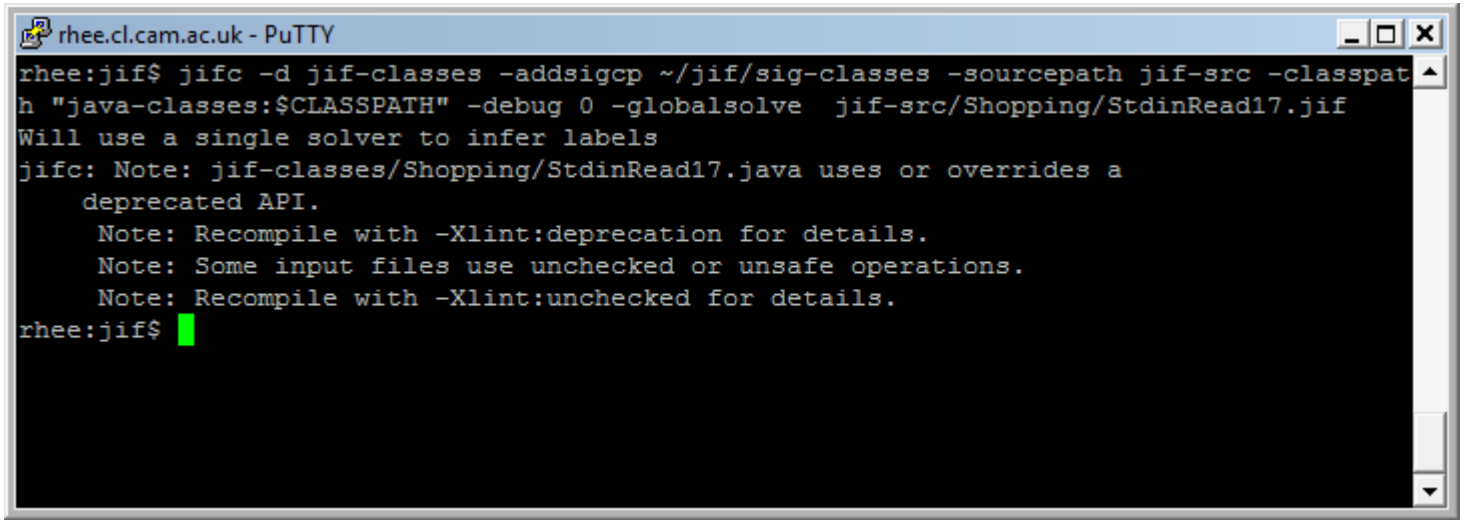
- **Literal:** String{pCustomer->pMarketing} sEmail = "sdp36@cl";
- **Dynamic:** final label lblEmail = new label {pCustomer->pMarketing};
  String{*lblEmail} sEmail = "sdp36@cl";
  String{sEmail} sTelephone = "763668";
- **Principal:** public static void main(String[] args, principal pp) {
  final principal pMarketing = new ExternalPrincipal("MD");
- **Runtime label ordering:** <= (less restrictive than)

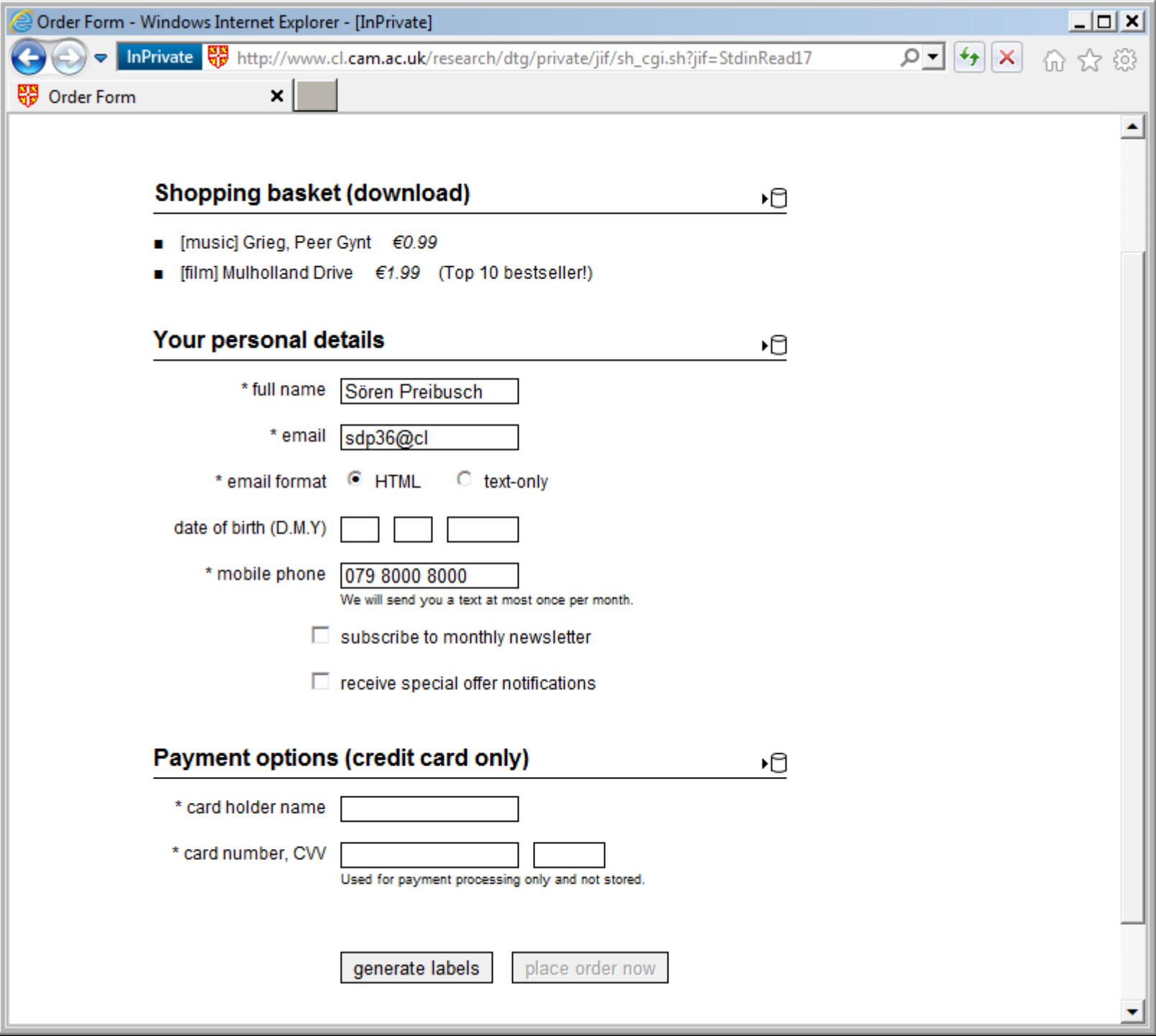
Runtime check: assertion at compile-time

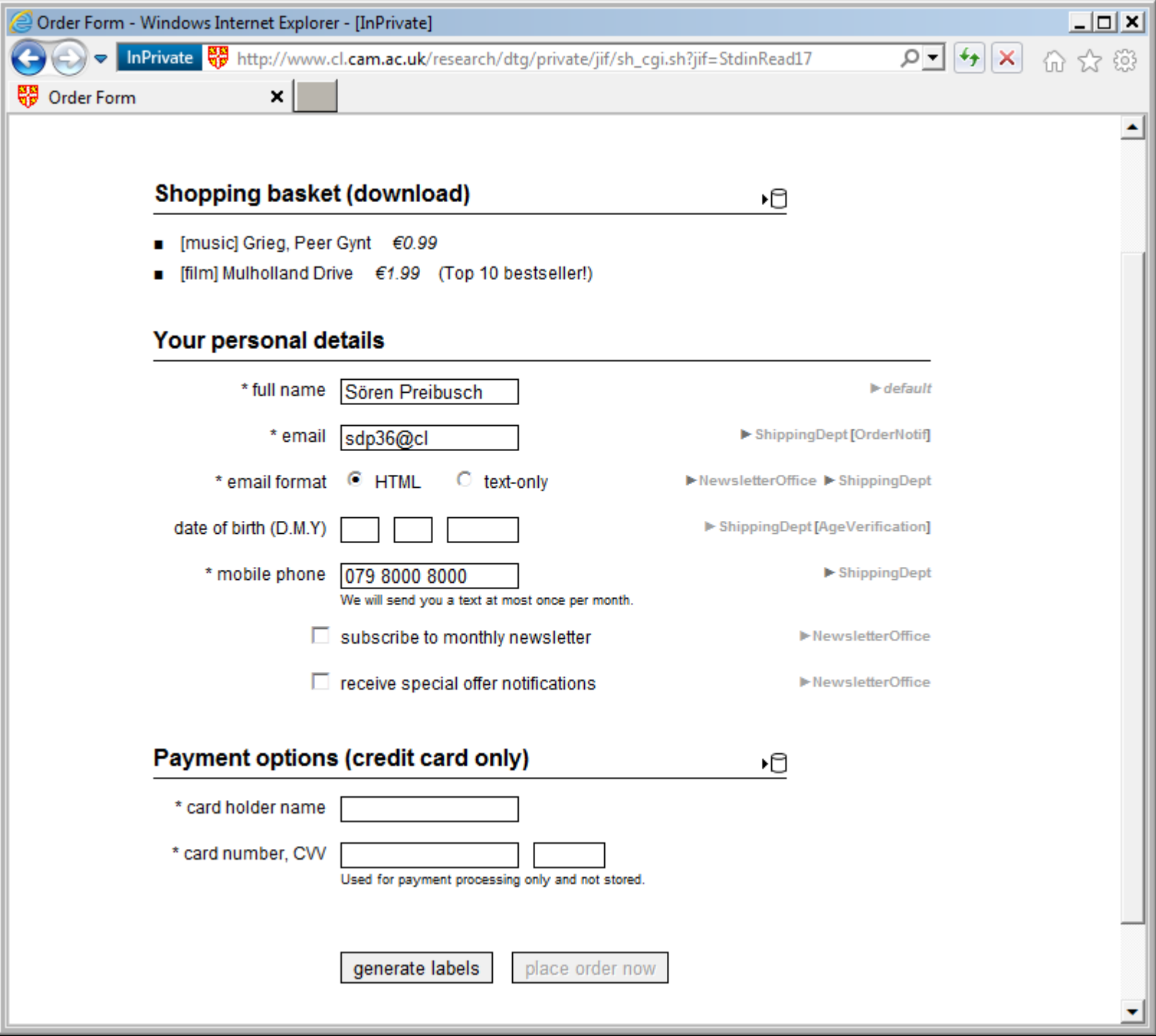
String{*lblNewsletter} sAddresses = " ";

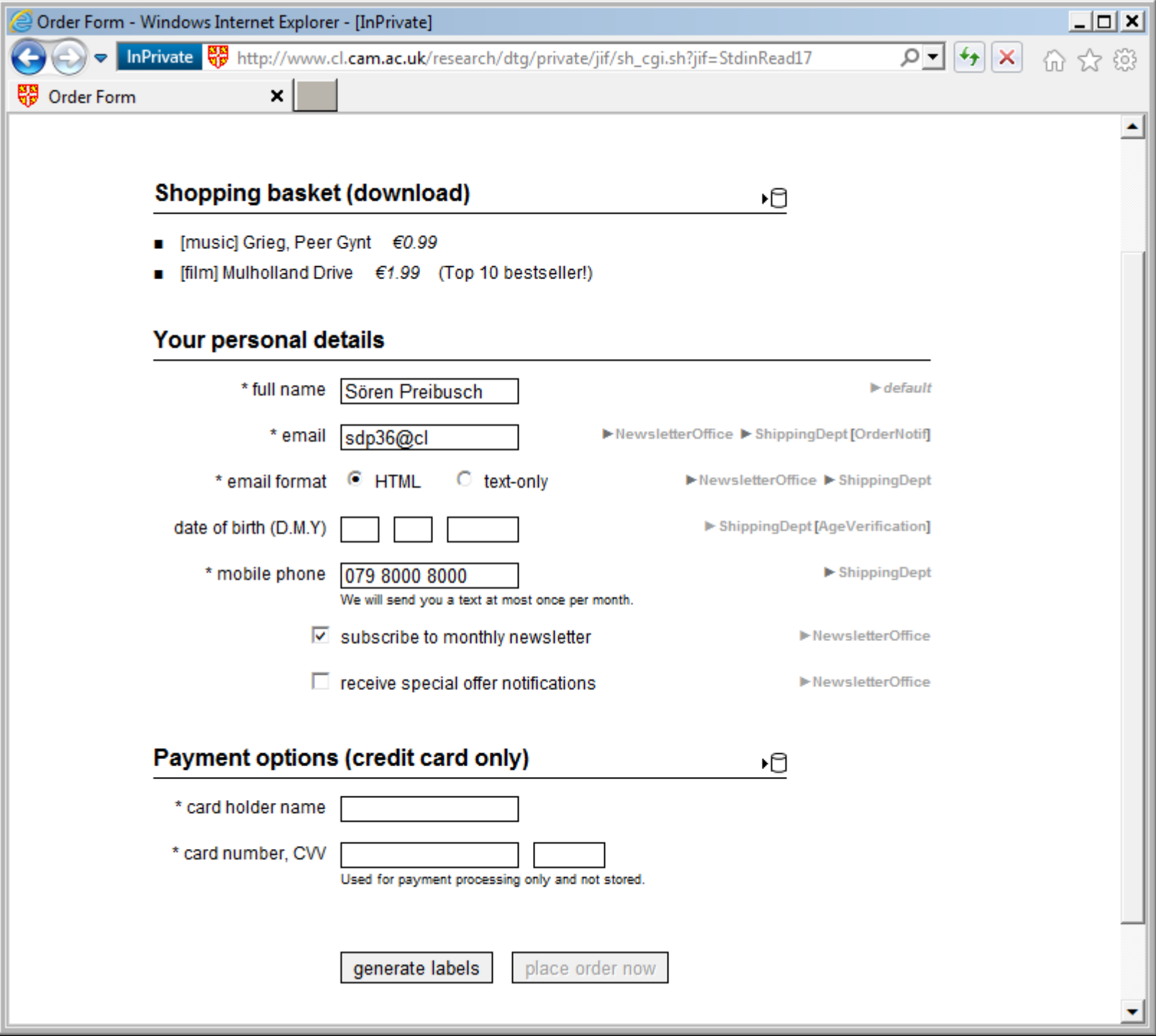
String{*lblEmail} sEmail = "sdp36@cl";

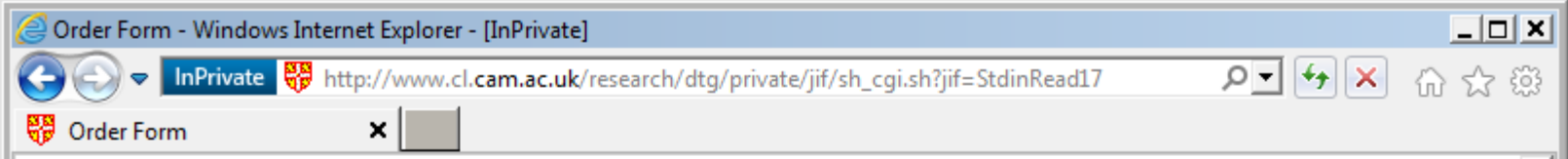
if(lblEmail <= lblNewsletter) sAddresses += sEmail;




Order Form - Windows Internet Explorer - [InPrivate]
InPrivate
http://www.cl.cam.ac.uk/research/dtg/private/jif/sh_cgi.sh?jif=StdinRead17
Order Form
Shopping basket (download)
[music] Grieg, Peer Gynt €0.99
[film] Mulholland Drive €1.99 (Top 10 bestseller!)
Your personal details
* full name
Sören Preibusch
* email
sdp36@cl
* email format
HTML
text-only
date of birth (D.M.Y)
* mobile phone
079 8000 8000
We will send you a text at most once per month.
subscribe to monthly newsletter
receive special offer notifications
Payment options (credit card only)
* card holder name
* card number, CVV
Used for payment processing only and not stored.
generate labels
place order now


Order Form - Windows Internet Explorer - [InPrivate]
InPrivate
http://www.cl.cam.ac.uk/research/dtg/private/jif/sh_cgi.sh?jif=StdinRead17
Order Form
Shopping basket (download)
[music] Grieg, Peer Gynt €0.99
[film] Mulholland Drive €1.99 (Top 10 bestseller!)
Your personal details
* full name
Sören Preibusch
default
* email
sdp36@cl
ShippingDept [OrderNotif]
* email format
HTML
text-only
NewsletterOffice
ShippingDept
date of birth (D.M.Y)
ShippingDept [AgeVerification]
* mobile phone
079 8000 8000
ShippingDept
We will send you a text at most once per month.
subscribe to monthly newsletter
NewsletterOffice
receive special offer notifications
NewsletterOffice
Payment options (credit card only)
* card holder name
* card number, CVV
Used for payment processing only and not stored.
generate labels
place order now


Order Form - Windows Internet Explorer - [InPrivate]
InPrivate
http://www.cl.cam.ac.uk/research/dtg/private/jif/sh_cgi.sh?jif=StdinRead17
Order Form
Shopping basket (download)
[music] Grieg, Peer Gynt €0.99
[film] Mulholland Drive €1.99 (Top 10 bestseller!)
Your personal details
* full name
Sören Preibusch
default
* email
sdp36@cl
NewsletterOffice ShippingDept [OrderNotif]
* email format
HTML
text-only
NewsletterOffice ShippingDept
date of birth (D.M.Y)
ShippingDept [AgeVerification]
* mobile phone
079 8000 8000
We will send you a text at most once per month.
ShippingDept
subscribe to monthly newsletter
NewsletterOffice
receive special offer notifications
NewsletterOffice
Payment options (credit card only)
* card holder name
* card number, CVV
Used for payment processing only and not stored.
generate labels
place order now



Uh-oh!

It seems you missed completing some of the mandatory fields.
Please review the form below.

Shopping basket (download)

- [music] Grieg, Peer Gynt *€0.99*
- [film] Mulholland Drive *€1.99* (Top 10 bestseller!)

Your personal details

* full name: Sören Preibusch

* email: sdp36@cl

* email format: (•) HTML ( ) text-only

date of birth (D.M.Y):

* mobile phone: 079 8000 8000

We will send you a text at most once per month.

[ ] subscribe to monthly newsletter

[ ] receive special offer notifications

Payment options (credit card only)

*** card holder name**

*** card number, CVV**

Used for payment processing only and not stored.

System architecture

<input name="email>ShippingDept[OrderNotif]" />

POST email>ShippingDept[OrderNotif]=sdp36@cl

parse into label: {pShip->pShip; pShip<-usageNotif}

Wrapper object for labelled data

```
final label lEmail = oEmail.getLabel();
String{*lEmail} sEmail = oEmail.getVal();

final principal usageNotif = new Usage("OrderNotif");
final NamedDataRecipient pShip = oPrinFactory.createRecipient("ShippingDept");

final label lRequShipNotif = new label {pShip->pShip; pShip<-usageNotif};
String{*lRequShipNotif} sQueueShipNotif = "";

if(lEmail <= lRequShipNotif)
    sQueueShipNotif += sEmail;
```

Usage extends AbstractPrincipal

Principal factory

Confidentiality; integrity policies
Recipient and usage constraints

Personal experience of programming in JIF

- **Long learning phase (frustration...)**
- **Plateau of productivity reached eventually**
  - Mostly pure Java coding then
  - After labelling and reordering control flow
- **Debugging nightmare**

Limitations

- **Systematic limitations**
  - generic label application
  - debugging
  - label signatures for runtime functions
- **Software engineering**
  - refactoring functionality
  - access modifiers
  - changes in output channels
  - no strict factory pattern
- **JIF limitations**
  - no Java generics
  - lacking documentation
  - method label signatures
  - label interoperability literal ↔ dynamic

Take-home message

- The JIF programming language is a powerful tool to engineer IFC-supported privacy compliance.
- Usability traps and systematic limitations are a major hindrance towards adoption.

Thank you very much.

Questions and comments

are welcome and highly appreciated.

sdp36@cl.cam.ac.uk

preibusch.de

privacy-calculus.net