

Interoperability Agreement

'Not – technical issues of IOP'

Second eEpoch Conference

Issy-les-Moulineaux

September 24, 2003

Theo van Sprundel

Schlumberger Cards



Agenda

- Introduction and background
- Basic choices
- Interoperability
- Agreement
 -
 -
 -
- How to continue ?



Focus and limitation

- Interoperability between 'entities'
 - Multi party
 - Multi application
 - Multi service
- 'Entities' being Card Scheme Operators / Card Issuers
- Mutual Legal questions
 - Responsibilities
 - Functional
 - Business / financial
- Manage positions / risks
 - Card holder and business entities
 - Technical equipments
 - Rights and obligation concerning services
 - Content ownership

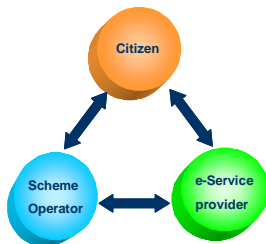
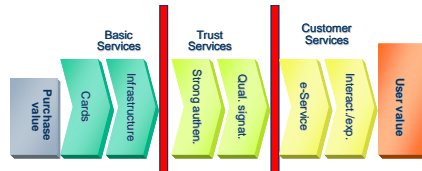
Why IOP agreements ?

- European Directives
- National Legislation
- A coherent set of agreements
 - Direct agreements between smart card schemes because of IOP
 - Card base
 - Services
 - Implied agreements between smart card schemes and 'its' roles
 - Card holders
 - Trust providers
 - E-service providers
 - Online agreements between card Service Providers and Card Holder

Strict modeling (1)

- Lines of demarcation

- Basic services
- Trust services
- E-Services



- Triangle of Trust

- Card scheme operator
- Service provider
- Card holder

Strict modeling (2)

- Roles and definitions

- Processes taxonomy

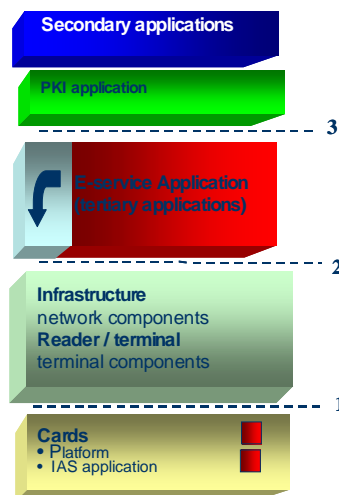
- Primary: IAS process
- Secondary: Conditional
- Tertiary: E-service

- Architecture model

- Cards
- Infrastructure
- Services
- Certificates

- Data and data flows

- I - A - S differentiation
- Entities and components
- Financial position
- E-services



What is 'interoperability' ?

IAS Services

- Arranged between one card scheme (on-us) and another (not on us)
 - Card "I welcome your card"
 - Infra structure "You may use my infrastructure"
 - E- Service " I offer you access to my e-services" / "You may offer your e-services my card base"
 - Certificate "I accept and trust your certificate check as my own"
- Conditions
 - Assessment "OK, my e-service providers can trust you"
 - Agreement "Contract, based on delegated responsibilities"
 - Operational checks "I secure all contracted processes"

Offering & Accepting side

Interoperability agreement content (1)



'I offer you the services of my providers !'

- Can you access the service ?
- Can you support operational security
- Can you read my IAS requirements ?
- Can you check my certificates ?
- Can we exchange session log data?

'You may use my card- base, infrastructure, certificates'

- Internet or presentation on local infrastructure
- Standards and operational checks
- Business rules file in e-service application + network
- OCSP or CRL.
- Invoicing

Interoperability agreement content (2)

“I welcome your cards/certs in my infrastructure”

- Can I read your card, and do the initial checks ?
- Can I read the IAS require-ments for the e-service
- How does my infrastructure assist the cert. check ?
- Your e-service applications on my infrastructure ?
- Can we exchange log data

“I offer my ambulant card-holders extra access”

- Global platform/ Java + opening specs
- Business rules file in the e-service application
- Agree about procedure
- Yes / No required
- Invoice

General Agreement Content

- Entities involved
- Preamble
- Definitions
- Objectives
- Interoperability
- Obligations
- Trust
- Accession
- Costs
- Problem handling
- Duration and termination

Appendices / side letters

- Processes
- Roles, entities, organization
- Architecture
- Card specs
- IAS/IOP interface
- Terminal specs
- Certificate specs
- Minimal data
- Testing and accepting procedures

Preamble

- Context
 - General
 - Having assessed and accepted the processes
- Intention: IAS interoperability
- Common technology Basis (smart cards, PKI, ..)
- Business rationale of the contract parties
 - in general
 - as delegated from underlying parties involved
- Position and status of underlying entities, including property and responsibility
- Legal references

Definitions / specifications

- Entities and Roles
- (Technical) Components
- Key words concerning standards
- Documents

Reference:

- GIF
- OSCIE

Objectives

- Deliver Interoperable Services on IAS to Card holders
 - Cards (welcoming not- on- us cards)
 - Infrastructure (offering not-on-us access to on us card base)
 - Services (only the file containing the required IAS rules)
 - Offering on us services to be accessed by not on us cards
 - Offering not-on-us services to on us card base
 - Certificate check at request of not on us services (always for on us cards)
- On behalf and interest of
 - Card acceptor / access provider
 - Certificate Validators
 - E- Service and Content providers

Interoperability services to be implemented (*)

- Card, with reference to
 - Type / standards - offered / accepted
 - Data
 - Infrastructure
 - Type / standards – offered / accepted
 - Emulation of non standard cards
 - Network services
 - E Services
 - Type of technology
 - Required rules file
 - PKI
 - Type of certificate check
- (*) Specified in side letters and all in compliance with appendix

Obligations

- Organization prerequisites
- Process as assessed
- Test interoperability
- Implement capability with technical components
- Implement Framework of contracts
- Code of conduct towards cardholders
- Alerting for problems

Trust

Unauthorized use / Obligations

- Contracts
 - Clear (communicated) separation of responsibility
 - Conditioned delegation
 - Confidentiality
- Conditioning processes
 - Card / cert issuing
 - Reliable e-services
 - Good Governance
- Operational processes

Accession

Open for new

- E-Service providers (*)
- Content providers (*)
- Card acceptors / access providers
- Card holders
- Certificate providers (*)

..... (*) with / without notification
with / without conditions / refusal,

Costs for interoperability services

Over 'Lines of demarcation':

- Initial costs
- Costs per period for service
- Direct costs (*)
 - Use of the card
 - Use of infrastructure
 - Use of a service
 - Use of a checked certificate



(*) Coordinated with log files

Problem handling

- Participate in coordination forum
- Notification of problems
- Implementing required enhancements
- Announcing legal procedures
- Arbitrage
- Jurisdiction

Duration and termination

- Starting / ending date
- Automatic continuation (per 3,6 12 month)
- Termination
- Automatic termination
 - Bankrupt of card issuer etc.
 - other cases
- Responsibility/claims after termination

How to continue ?

- Next steps
 - Task force to define the agreement model
 - General MOU in which the model is implied
 - experts team for 'technical annex'
- Conference 3
 - Acceptance
 - Implementation per pair of pilots
- References
 - OSCIE V2, volume 5, part 1 (TB 7)
 - MOU Finland / Estonia
 - Netcards

Thank you for you kind attention !

Theo van Sprundel
Schlumberger Cards
Weesp (The Netherlands)
Tel. 0031 294 239 546 (office)
0031 655 888 247 (mobile)
Tsprundel@slb.com