Domain Specific Formal Languages

– A Calculus for Orchestration of Web Services –

Francesco Tiezzi

School of Science and Technology

Computer Science Division

University of Camerino

A.A. 2016/2017

Motivation

Deficiency

Current software engineering technologies for SOC

- remain at a linguistic level
- do not support analytical tools for checking that SOC applications enjoy desirable correctness properties

Goal

Develop *formal reasoning mechanisms* and *analytical tools* for checking that services (possibly resulting from a *composition*) meet desirable properties and do not manifest unexpected behaviors

Motivation

Deficiency

Current software engineering technologies for SOC

- remain at a linguistic level
- do not support analytical tools for checking that SOC applications enjoy desirable correctness properties

Goal

Develop *formal reasoning mechanisms* and *analytical tools* for checking that services (possibly resulting from a *composition*) meet desirable properties and do not manifest unexpected behaviors

Approach

Goal

Developing *formal reasoning mechanisms* and *analytical tools* for checking that the services resulting from a *composition* meet desirable correctness properties and do not manifest unexpected behaviors

Approach: rely on Process Calculi

- Convey in a distilled form the paradigm at the heart of SOC (being defined algebraically, they are inherently compositional)
- Provide linguistic formalisms for description of service-based applications and their composition
- Hand down a large set of reasoning mechanisms and analytical tools, e.g. typing systems and model checkers

Approach

Goal

Developing *formal reasoning mechanisms* and *analytical tools* for checking that the services resulting from a *composition* meet desirable correctness properties and do not manifest unexpected behaviors

Approach: rely on Process Calculi

- Convey in a distilled form the paradigm at the heart of SOC (being defined algebraically, they are inherently compositional)
- Provide linguistic formalisms for description of service-based applications and their composition
- Hand down a large set of reasoning mechanisms and analytical tools, e.g. typing systems and model checkers

Process Calculi for SOC

- To model service composition, many process calculi-like formalisms have been designed
- Most of them only consider a few specific features separately, possibly by embedding ‘ad hoc’ constructs within some well-studied process calculus
  (e.g., the variants of CSP/π-calculus with transactions)
- One major goal is assessing the adequacy of diverse sets of primitives w.r.t. modelling, combining and analysing service-oriented systems

Process Calculi for SOC: an overview

Process calculi for SOC can be classified according to the approach used for maintaining the link between *caller* and *callee*

- **Sessions**: the link is determined by a private channel that is implicitly created when the first message exchange of a conversation takes place
- **Correlations**: the link is determined by correlation values included in the exchanged messages
- **No link**: some works do not take into account this aspect e.g. $\mathtt{web}\pi$, $\mathtt{web}\pi_\infty$, CSP/π-calculus + transactions, ...

Process Calculi for SOC: an overview

Process calculi for SOC can be classified according to the approach used for maintaining the link between *caller* and *callee*

- **Sessions**: the link is determined by a private channel that is implicitly created when the first message exchange of a conversation takes place

- **Correlations**: the link is determined by correlation values included in the exchanged messages

- **No link**: some works do not take into account this aspect e.g. $\mathtt{web}\pi$, $\mathtt{web}\pi_\infty$, CSP/π-calculus + transactions, …

Process Calculi for SOC: an overview

Process calculi for SOC can be classified according to the approach to maintain the link between *caller* and *callee*

- **Sessions**: the link is determined by a private channel that is implicitly created when the first message exchange of a conversation takes place
  - *dyadic*: they can be further grouped according to the inter-session communication mechanism
    - CaSPiS: dataflow communication
    - SSCC: stream-based communication
    - π-calculus + sessions (in many works): session delegation
  - *multiparty*:
    - Conversation Calculus, μse, π-calculus + (asynchronous/synchronous) multiparty sessions
- **Correlations**: the link is determined by correlation values included in the exchanged messages
  - *stateful*: every service instance has an explicit state
    - WS-CALCULUS
    - SOCK
  - *stateless*: state is not explicitly modelled
    - COWS

Process Calculi for SOC: an overview

Process calculi for SOC can be classified according to the approach to maintain the link between *caller* and *callee*

- **Sessions**: the link is determined by a private channel that is implicitly created when the first message exchange of a conversation takes place
  - *dyadic*: they can be further grouped according to the inter-session communication mechanism
    - CASPIS: dataflow communication
    - SSCC: stream-based communication
    - π-calculus + sessions (in many works): delegation
  - *multiparty*:
    - Conversation Calculus, μse
    - π-calculus + (asynchronous/synchronous) multiparty sessions
- **Correlations**: the link is determined by correlation values included in the exchanged messages
  - *stateful*: every service instance has an explicit state
    - WS-CALCULUS
    - SOCK
  - *stateless*: state is not explicitly modelled
    - COWS

Process Calculi for SOC: an overview

Process calculi for SOC can be classified according to the approach to maintain the link between *caller* and *callee*

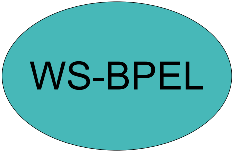
- **Sessions**: the link is determined by a private channel that is implicitly created when the first message exchange of a conversation takes place
- **Correlations**: the link is determined by correlation values included in the exchanged messages
  - ★ *stateful*: every service instance has an explicit state
    - WS-CALCULUS
    - SOCK
  - ★ *stateless*: state is not explicitly modelled
    - COWS

COWS [ESOP'07]

A process calculus for specifying and combining service-oriented applications, while modelling their dynamic behaviour

An introduction to COWS

COWS: a Calculus for Orchestration of Web Services

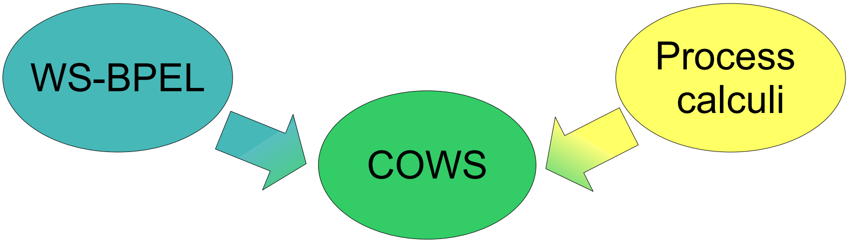


- Inspired by
  - the OASIS standard WS-BPEL for WS orchestration
  - previous work on process calculi
- Indeed, COWS intends to be a foundational model not specifically tight to Web services' current technologies
- COWS combines in an original way a number of constructs and features borrowed from well-known process calculi

COWS: a Calculus for Orchestration of Web Services

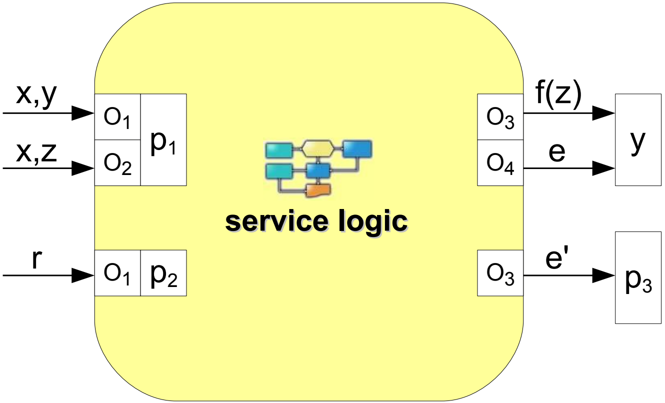
- Inspired by
  - the OASIS standard WS-BPEL for WS orchestration
  - previous work on process calculi
- Indeed, COWS intends to be a foundational model not specifically tight to Web services' current technologies
- COWS combines in an original way a number of constructs and features borrowed from well-known process calculi

COWS: a Calculus for Orchestration of Web Services

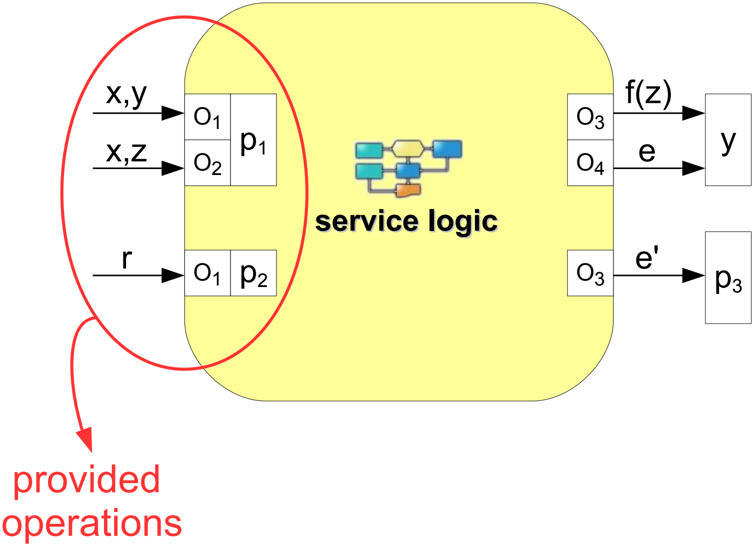


- Inspired by
  - the OASIS standard WS-BPEL for WS orchestration
  - previous work on process calculi
- Indeed, COWS intends to be a foundational model not specifically tight to Web services' current technologies
- COWS combines in an original way a number of constructs and features borrowed from well-known process calculi

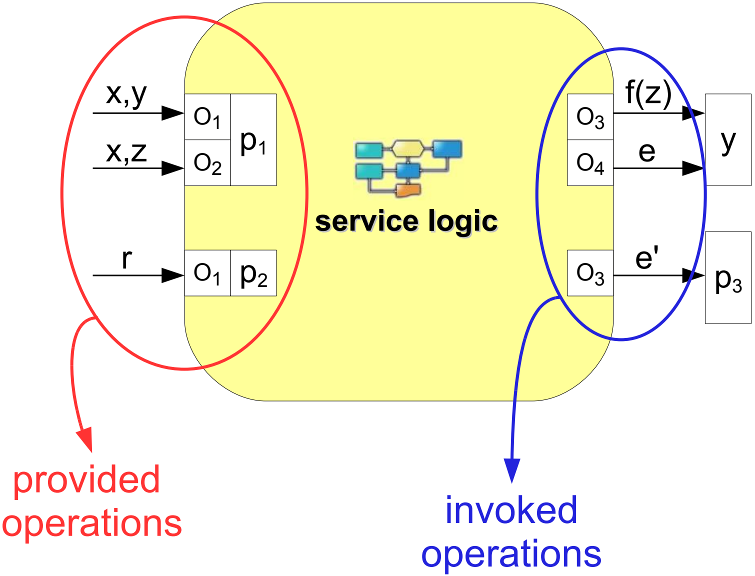
The notion of service in COWS



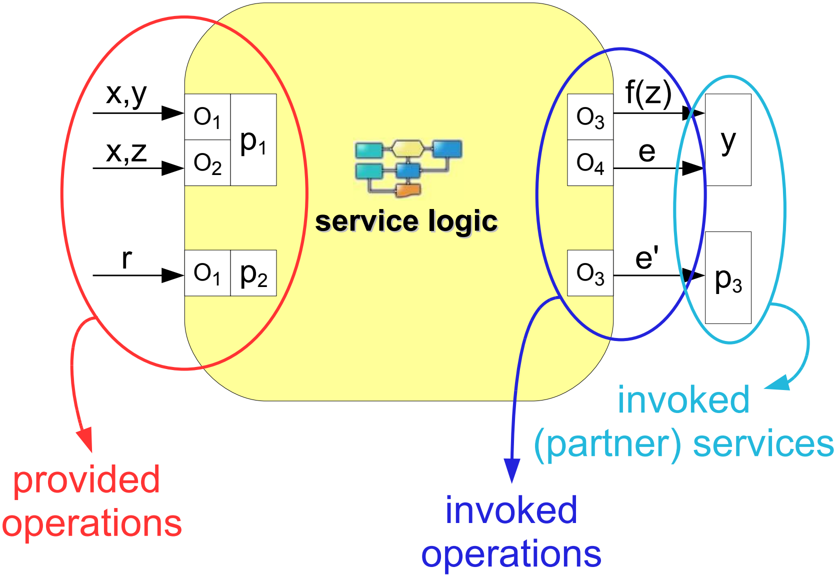
The notion of service in COWS



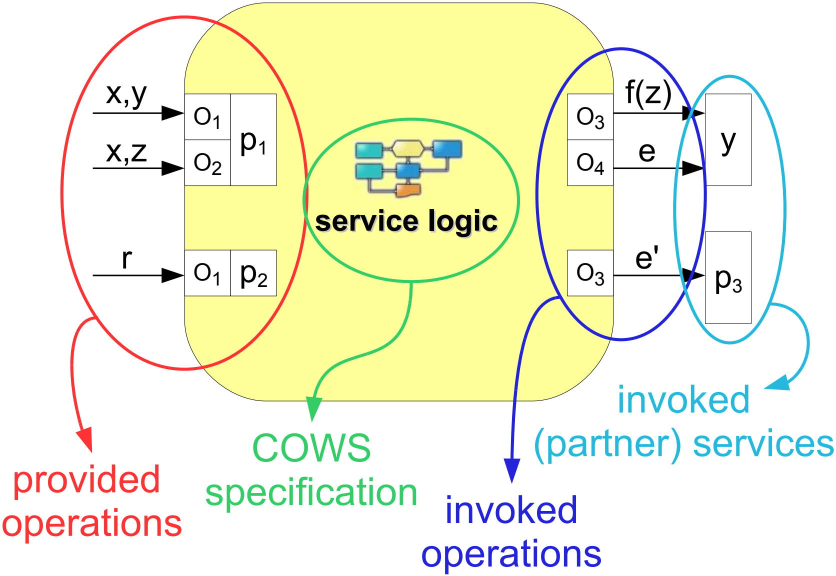
The notion of service in COWS



The notion of service in COWS



The notion of service in COWS



COWS in three steps

μCOWS^m (micro COWS minus priority)

Communication activities

- Invoke
- Receive

Control flow activities

- Parallel composition
- Replication
- Choice
- Delimitation

COWS in three steps

μCOWS^m (micro COWS minus priority)

Communication activities

- Invoke
- Receive

Control flow activities

- Parallel composition
- Choice
- Replication
- Delimitation

- Priority in the parallel composition

COWS in three steps

μCOWS (micro COWS)

μCOWS^m (micro COWS minus priority)

Communication activities

- Invoke
- Receive

Control flow activities

- Parallel composition
- Choice
- Replication
- Delimitation

- Priority in the parallel composition

COWS in three steps

μCOWS (micro COWS)

μCOWS^m (micro COWS minus priority)

Communication activities

- Invoke
- Receive

Control flow activities

- Parallel composition
- Choice
- Replication
- Delimitation

- Priority in the parallel composition

Termination activities

- Kill activity
- Protection

COWS in three steps

COWS (Calculus for Orchestration of Web Services)

μCOWS (micro COWS)

μCOWS^m (micro COWS minus priority)

Communication activities

- Invoke
- Receive

Control flow activities

- Parallel composition
- Choice
- Replication
- Delimitation

- Priority in the parallel composition

Termination activities

- Kill activity
- Protection

Syntax of μCOWS^m

$s ::=$		(services)
	$u \bullet u' ! \bar{\epsilon}$	(invoke)
$\mid$	$\sum_{i=0}^{r} g_i . s_i$	(receive-guarded choice)
$\mid$	$s \mid s$	(parallel composition)
$\mid$	$[u]\, s$	(delimitation)
$\mid$	$* s$	(replication)
$g ::=$		(guards)
	$p \bullet o ? \bar{w}$	(receive)

(notations)
ϵ: *expressions*
x: *variables*
v: *values*
n, p, o: *names*
u: *variables* | *names*
w: *variables* | *values*

μCOWS^m vs. π-calculus, fusion, Value-passing CCS, Dπ, ...

$$\left.\begin{array}{l} \bullet \text{ asynchronous and polyadic communication} \\ \bullet \text{ input} - \text{guarded choice} \\ \bullet \text{ polyadic synchronization} \\ \bullet \text{ localised channels} \end{array}\right\} \pi\text{-calculus}$$

$$\bullet \text{ global scoping (and non} - \text{binding input)} \quad \} \text{ fusion}$$

$$\bullet \text{ distinction between variables and values} \quad \} \text{ vp CCS, App. } \pi\text{-calculus, D}\pi$$

$$\bullet \text{ pattern} - \text{matching} \quad \} \text{ Klaim}$$

Syntax of μCOWS^m

$s ::=$		(services)
	$u \bullet u' ! \bar{\epsilon}$	(invoke)
$\mid$	$\sum_{i=0}^{r} g_i . s_i$	(receive-guarded choice)
$\mid$	$s \mid s$	(parallel composition)
$\mid$	$[u]\, s$	(delimitation)
$\mid$	$* \, s$	(replication)
$g ::=$		(guards)
	$p \bullet o ? \bar{w}$	(receive)

(notations)
ϵ: *expressions*
x: *variables*
v: *values*
n, p, o: *names*
u: *variables* | *names*
w: *variables* | *values*

Notations

- The exact syntax of expressions is deliberately omitted
- $\bar{\ }$ denotes tuples of objects, e.g. $\bar{w}$ is a tuple of variables and/or values

Syntax of μCOWS^m

$s ::=$		(services)
	$u \bullet u' ! \bar{\epsilon}$	(invoke)
$\mid$	$\sum_{i=0}^{r} g_i . s_i$	(receive-guarded choice)
$\mid$	$s \mid s$	(parallel composition)
$\mid$	$[u]\, s$	(delimitation)
$\mid$	$* \, s$	(replication)
$g ::=$		(guards)
	$p \bullet o ? \bar{w}$	(receive)

(notations)
ϵ: *expressions*
x: *variables*
v: *values*
n, p, o: *names*
u: *variables* | *names*
w: *variables* | *values*

Communication activities

- Services are provided and invoked through communication *endpoints*, written as $p \bullet o$ (i.e. 'partner name' plus 'operation name')
- Receive activities bind neither names nor variables
- Communication is regulated by *pattern-matching*
- Partner names and operation names can be exchanged when communicating (only the 'send capability' is passed over)
- Communication is asynchronous

Syntax of μCOWS^m

$$
\begin{array}{lll}
s ::= & & \text{(services)} \\
& u \bullet u'!\bar{\epsilon} & \quad \text{(invoke)} \\
| & \sum_{i=0}^{r} g_i . s_i & \quad \text{(receive-guarded choice)} \\
| & s \mid s & \quad \text{(parallel composition)} \\
| & [u]\, s & \quad \text{(delimitation)} \\
| & * \, s & \quad \text{(replication)} \\
g ::= & & \text{(guards)} \\
& p \bullet o?\bar{w} & \quad \text{(receive)}
\end{array}
$$

(notations)
ϵ: *expressions*
x: *variables*
v: *values*
n, p, o: *names*
u: *variables* | *names*
w: *variables* | *values*

Choice

- $+$ abbreviates binary choice, while empty choice will be denoted by **0**

Syntax of μCOWS^m

$s ::=$		(services)
	$u \bullet u' ! \bar{\epsilon}$	(invoke)
$\mid$	$\sum_{i=0}^{r} g_i . s_i$	(receive-guarded choice)
$\mid$	$s \mid s$	(parallel composition)
$\mid$	$[u]\, s$	(delimitation)
$\mid$	$* \, s$	(replication)
$g ::=$		(guards)
	$p \bullet o ? \bar{w}$	(receive)

(notations)
ϵ: *expressions*
x: *variables*
v: *values*
n, p, o: *names*
u: *variables* | *names*
w: *variables* | *values*

Parallel composition

- Permits interleaving executions of activities

Syntax of μCOWS^m

$$
\begin{array}{rlll}
s ::= & & & \text{(services)} \\
& & u \bullet u'!\bar{\epsilon} & \text{(invoke)} \\
& | & \sum_{i=0}^{r} g_i . s_i & \text{(receive-guarded choice)} \\
& | & s \mid s & \text{(parallel composition)} \\
& | & [u]\, s & \text{(delimitation)} \\
& | & * \, s & \text{(replication)} \\
g ::= & & & \text{(guards)} \\
& & p \bullet o?\bar{w} & \text{(receive)}
\end{array}
$$

(notations)
ϵ: *expressions*
x: *variables*
v: *values*
n, p, o: *names*
u: *variables* | *names*
w: *variables* | *values*

Delimitation

- Only one binding construct: $[u]\, s$ binds u in the scope s
  - free/bound names and variables and closed terms defined accordingly
- Delimitation is used to:
  1. regulate the range of application of substitutions
  2. generate fresh names

Syntax of μCOWS^m

$s ::=$		(services)
	$u \bullet u' ! \bar{\epsilon}$	(invoke)
$\mid$	$\sum_{i=0}^{r} g_i . s_i$	(receive-guarded choice)
$\mid$	$s \mid s$	(parallel composition)
$\mid$	$[u]\, s$	(delimitation)
$\mid$	$* \, s$	(replication)
$g ::=$		(guards)
	$p \bullet o ? \bar{w}$	(receive)

(notations)
ϵ: *expressions*
x: *variables*
v: *values*
n, p, o: *names*
u: *variables* | *names*
w: *variables* | *values*

Replication

- Permits implementing persistent services and recursive behaviours

μCOWS^m operational semantics

Labelled transition relation $\xrightarrow{\alpha}$

Label α is generated by the following grammar:

$$\alpha \quad ::= \quad \mathrm{n} \lhd \bar{v} \quad | \quad \mathrm{n} \rhd \bar{w} \quad | \quad \sigma$$

where σ is a *substitution*

i.e. a function from variables to values (written as collections of pairs $x \mapsto v$)

and n denotes endpoints (i.e. $p \bullet o$)

Structural congruence $\equiv$

Standard laws for $\sum$, $|$ and $*$, plus:

- $[u]\,\mathbf{0} \;\equiv\; \mathbf{0}$
- $[u_1]\,[u_2]\,s \;\equiv\; [u_2]\,[u_1]\,s$
- $s_1 \mid [u]\,s_2 \;\equiv\; [u]\,(s_1 \mid s_2)$ if $u \notin \mathrm{fu}(s_1)$

  $\mathrm{fu}(s)$ denotes the set of elements occurring free in s

μCOWS^m operational semantics

Labelled transition relation $\xrightarrow{\alpha}$

Label α is generated by the following grammar:

$$\alpha \quad ::= \quad \mathrm{n} \lhd \bar{v} \quad | \quad \mathrm{n} \rhd \bar{w} \quad | \quad \sigma$$

where σ is a *substitution*

i.e. a function from variables to values (written as collections of pairs $x \mapsto v$)

and n denotes endpoints (i.e. $p \bullet o$)

Structural congruence $\equiv$

Standard laws for $\sum$, $|$ and $*$, plus:

- $[u]\,\mathbf{0} \equiv \mathbf{0}$
- $[u_1]\,[u_2]\,s \equiv [u_2]\,[u_1]\,s$
- $s_1 \mid [u]\,s_2 \equiv [u]\,(s_1 \mid s_2)$ if $u \notin \mathrm{fu}(s_1)$

  $\mathrm{fu}(s)$ denotes the set of elements occurring free in s

μCOWS^m: Invoke/receive activities & Choice

Invoke activities

- Can proceed only if the expressions in the argument can be evaluated
- *Evaluation function* $[\![\_]\!]$: takes closed expressions and returns values

$$\frac{[\![\bar{\epsilon}]\!] = \bar{v}}{\mathrm{n}!\bar{\epsilon} \xrightarrow{\mathrm{n} \lhd \bar{v}} \mathbf{0}}$$

Choice (among receive activities)

- Offers an alternative choice of endpoints
- It is *not* a binder for names and variables (delimitation is used to delimit their scope)

$$\sum_{i=1}^{r} \mathrm{n}_i?\bar{w}_i.s_i \xrightarrow{\mathrm{n}_j \rhd \bar{w}_j} s_j \qquad (1 \leq j \leq r)$$

μCOWS^m: Parallel composition

- Communication takes place when two parallel services perform matching receive and invoke activities

$$\frac{s_1 \xrightarrow{\mathrm{n} \triangleright \bar{w}} s_1' \qquad s_2 \xrightarrow{\mathrm{n} \triangleleft \bar{v}} s_2' \qquad \mathcal{M}(\bar{w}, \bar{v}) = \sigma}{s_1 \mid s_2 \xrightarrow{\sigma} s_1' \mid s_2'}$$

- Execution of parallel services is interleaved

$$\frac{s_1 \xrightarrow{\alpha} s_1'}{s_1 \mid s_2 \xrightarrow{\alpha} s_1' \mid s_2}$$

Matching function

$$\mathcal{M}(x, v) = \{x \mapsto v\} \qquad \mathcal{M}(v, v) = \emptyset \qquad \mathcal{M}(\langle\rangle, \langle\rangle) = \emptyset$$

$$\frac{\mathcal{M}(w_1, v_1) = \sigma_1 \quad \mathcal{M}(\bar{w}_2, \bar{v}_2) = \sigma_2}{\mathcal{M}((w_1, \bar{w}_2), (v_1, \bar{v}_2)) = \sigma_1 \uplus \sigma_2}$$

μCOWS^m: Parallel composition

- Communication takes place when two parallel services perform matching receive and invoke activities

$$\frac{s_1 \xrightarrow{\mathrm{n} \rhd \bar{w}} s_1' \qquad s_2 \xrightarrow{\mathrm{n} \lhd \bar{v}} s_2' \qquad \mathcal{M}(\bar{w}, \bar{v}) = \sigma}{s_1 \mid s_2 \xrightarrow{\sigma} s_1' \mid s_2'}$$

- Execution of parallel services is interleaved

$$\frac{s_1 \xrightarrow{\alpha} s_1'}{s_1 \mid s_2 \xrightarrow{\alpha} s_1' \mid s_2}$$

Matching function

$$\mathcal{M}(x, v) = \{x \mapsto v\} \qquad \begin{array}{l} \mathcal{M}(v, v) = \emptyset \\ \mathcal{M}(\langle\rangle, \langle\rangle) = \emptyset \end{array} \qquad \frac{\mathcal{M}(w_1, v_1) = \sigma_1 \quad \mathcal{M}(\bar{w}_2, \bar{v}_2) = \sigma_2}{\mathcal{M}((w_1, \bar{w}_2), (v_1, \bar{v}_2)) = \sigma_1 \uplus \sigma_2}$$

μCOWS^m: Parallel composition

- Communication takes place when two parallel services perform matching receive and invoke activities

$$\frac{s_1 \xrightarrow{\mathtt{n} \triangleright \bar{w}} s_1' \qquad s_2 \xrightarrow{\mathtt{n} \triangleleft \bar{v}} s_2' \qquad \mathcal{M}(\bar{w}, \bar{v}) = \sigma}{s_1 \mid s_2 \xrightarrow{\sigma} s_1' \mid s_2'}$$

- Execution of parallel services is interleaved

$$\frac{s_1 \xrightarrow{\alpha} s_1'}{s_1 \mid s_2 \xrightarrow{\alpha} s_1' \mid s_2}$$

Matching function

$$\mathcal{M}(x, v) = \{x \mapsto v\} \qquad \mathcal{M}(v, v) = \emptyset \qquad \mathcal{M}(\langle\rangle, \langle\rangle) = \emptyset \qquad \frac{\mathcal{M}(w_1, v_1) = \sigma_1 \quad \mathcal{M}(\bar{w}_2, \bar{v}_2) = \sigma_2}{\mathcal{M}((w_1, \bar{w}_2), (v_1, \bar{v}_2)) = \sigma_1 \uplus \sigma_2}$$

μCOWS^m: Delimitation

- $[u]\, s$ behaves like s, except when the transition label α contains u
- When the whole scope of a variable x is determined, and a communication involving x within that scope is taking place the delimitation is removed and the substitution for x is performed

$$\frac{s \xrightarrow{\alpha} s' \quad u \notin \mathrm{u}(\alpha)}{[u]\, s \xrightarrow{\alpha} [u]\, s'} \qquad \frac{s \xrightarrow{\sigma \uplus \{x \mapsto v\}} s'}{[x]\, s \xrightarrow{\sigma} s' \cdot \{x \mapsto v\}}$$

Substitutions (ranged over by σ):

- functions from variables to values (written as collections of pairs $x \mapsto v$)
- $\sigma_1 \uplus \sigma_2$ denotes the union of σ_1 and σ_2 when they have disjoint domains

$\mathrm{u}(\alpha)$ avoids capturing endpoints of actual communications,
it denotes the set of elements occurring in α,

μCOWS^m operational semantics

Labelled transition rules

$$\frac{[\![\bar{\epsilon}]\!] = \bar{v}}{\mathrm{n}!\bar{\epsilon} \xrightarrow{\mathrm{n} \lhd \bar{v}} \mathbf{0}}$$

$$\frac{1 \le j \le r}{\sum_{i=1}^{r} \mathrm{n}_i?\bar{w}_i.s_i \xrightarrow{\mathrm{n}_j \rhd \bar{w}_j} s_j}$$

$$\frac{s_1 \xrightarrow{\mathrm{n} \rhd \bar{w}} s_1' \qquad s_2 \xrightarrow{\mathrm{n} \lhd \bar{v}} s_2' \qquad \mathcal{M}(\bar{w}, \bar{v}) = \sigma}{s_1 \mid s_2 \xrightarrow{\sigma} s_1' \mid s_2'}$$

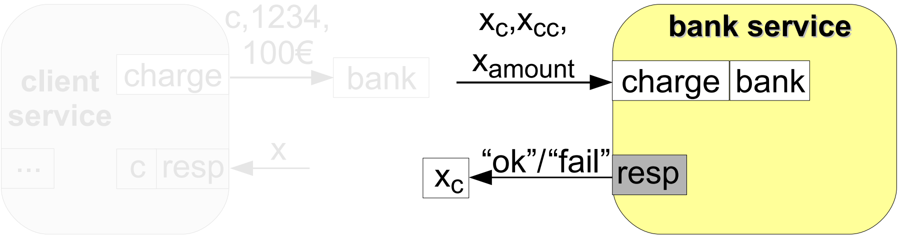
$$\frac{s_1 \xrightarrow{\alpha} s_1'}{s_1 \mid s_2 \xrightarrow{\alpha} s_1' \mid s_2}$$

$$\frac{s \xrightarrow{\sigma \uplus \{x \mapsto v\}} s'}{[x]\, s \xrightarrow{\sigma} s' \cdot \{x \mapsto v\}}$$

$$\frac{s \xrightarrow{\alpha} s' \quad u \notin \mathrm{u}(\alpha)}{[u]\, s \xrightarrow{\alpha} [u]\, s'}$$

$$\frac{s \equiv \xrightarrow{\alpha} \equiv s'}{s \xrightarrow{\alpha} s'}$$

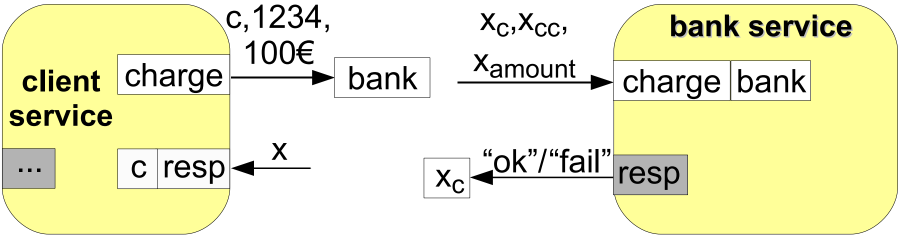
μCOWS^m: *simple* bank service example



$\mathsf{bank} \bullet \mathsf{charge}!\langle \mathsf{c}, 1234, 100€ \rangle$
$\mid [\mathsf{x}]\, (\mathsf{c} \bullet \mathsf{resp}?\langle \mathsf{x} \rangle.s \mid s')$

$[\mathsf{x_c}, \mathsf{x_{cc}}, \mathsf{x_{amount}}]$
$\mathsf{bank} \bullet \mathsf{charge}?\langle \mathsf{x_c}, \mathsf{x_{cc}}, \mathsf{x_{amount}} \rangle.$
$\mathsf{x_c} \bullet \mathsf{resp}!\langle chk(x_{cc}, x_{amount}) \rangle$

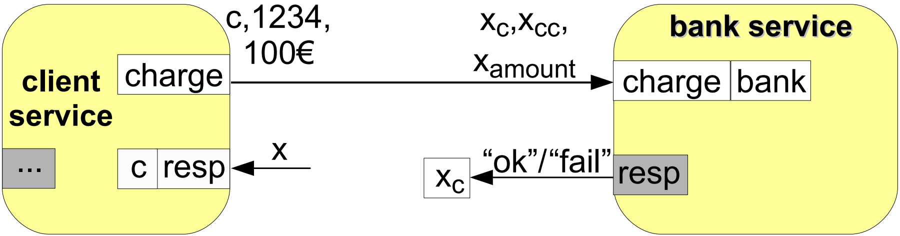
μCOWS^m: *simple* bank service example



$\mathsf{bank} \bullet \mathsf{charge}!\langle \mathsf{c}, 1234, 100€\rangle$
$\mid [\mathsf{x}]\,(\mathsf{c} \bullet \mathsf{resp}?\langle \mathsf{x}\rangle.\mathsf{s} \mid \mathsf{s}')$

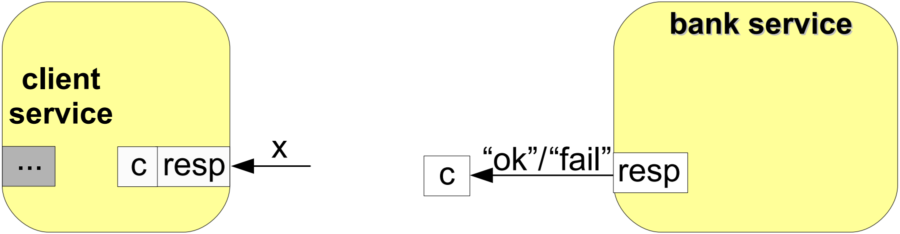
$[\mathsf{x_c}, \mathsf{x_{cc}}, \mathsf{x_{amount}}]$
$\mathsf{bank} \bullet \mathsf{charge}?\langle \mathsf{x_c}, \mathsf{x_{cc}}, \mathsf{x_{amount}}\rangle.$
$\mathsf{x_c} \bullet \mathsf{resp}!\langle chk(x_{cc}, x_{amount})\rangle$

μCOWS^m: *simple* bank service example



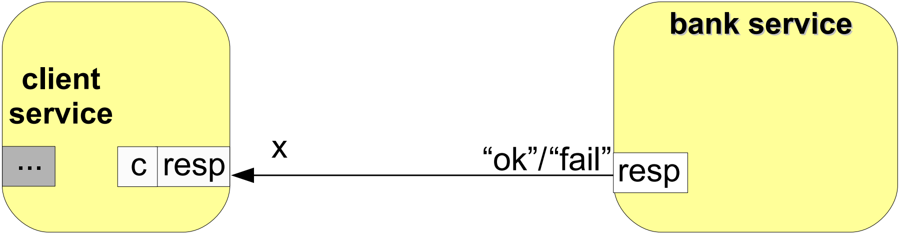
$$\mathsf{bank} \bullet \mathsf{charge}!\langle \mathsf{c}, 1234, 100€ \rangle \mid [\mathsf{x}]\,(\mathsf{c} \bullet \mathsf{resp}?\langle \mathsf{x} \rangle.\mathsf{s} \mid \mathsf{s}') \quad \mid \quad [\mathsf{x_c}, \mathsf{x_{cc}}, \mathsf{x_{amount}}]\ \mathsf{bank} \bullet \mathsf{charge}?\langle \mathsf{x_c}, \mathsf{x_{cc}}, \mathsf{x_{amount}} \rangle.\ \mathsf{x_c} \bullet \mathsf{resp}!\langle chk(x_{cc}, x_{amount}) \rangle$$

μCOWS^m: *simple* bank service example



$$[x]\,(c \bullet resp?\langle x\rangle.s \mid s') \qquad\qquad \mid \qquad\qquad c \bullet resp!\langle \mathit{chk}(1234, 100€)\rangle$$

μCOWS^m: *simple* bank service example

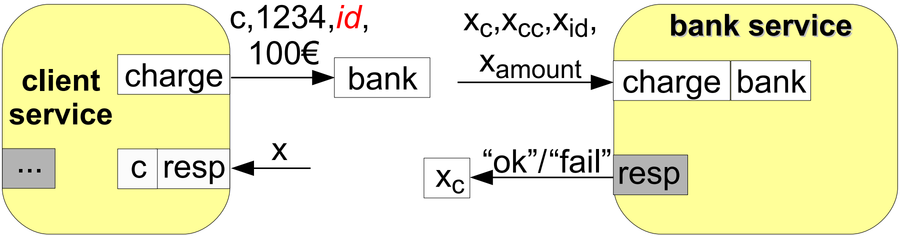


$$[x]\,(c \bullet \mathrm{resp}?\langle x\rangle.s \mid s') \quad \mid \quad c \bullet \mathrm{resp}!\langle \mathit{chk}(1234, 100€)\rangle$$

μCOWS^m: *simple* bank service example

$$(s \mid s') \cdot \{x \mapsto \text{“ok”} / \text{“fail”}\} \qquad \mid \qquad \mathbf{0}$$

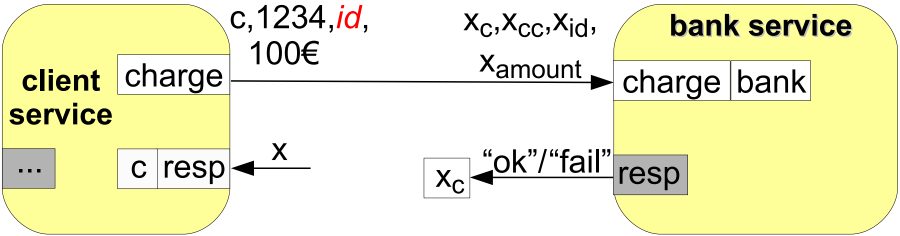
μCOWS^m: communication of private names



$[id]$
$(bank \bullet charge!\langle c, 1234, id, 100€\rangle$
$\mid [x]\,(c \bullet resp?\langle x\rangle.s \mid s')\,)$

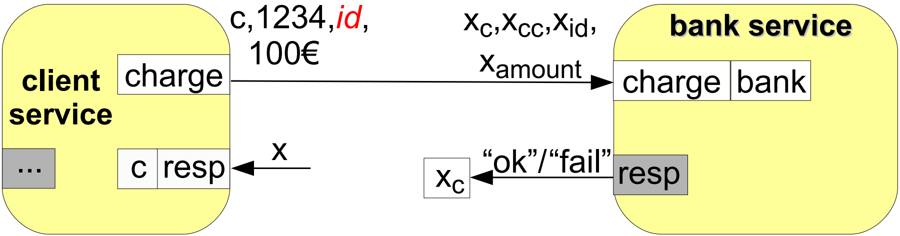
$[x_c, x_{cc}, x_{id}, x_{amount}]$
$bank \bullet charge?\langle x_c, x_{cc}, x_{id}, x_{amount}\rangle.$
$x_c \bullet resp!\langle chk(x_{cc}, x_{id}, x_{amount})\rangle$

μCOWS^m: communication of private names



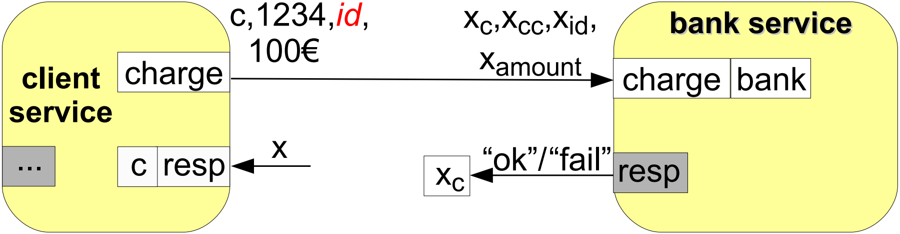
$$[id]\,(bank \bullet charge!\langle c, 1234, id, 100€\rangle \;\; | \;\; [x]\,(c \bullet resp?\langle x\rangle.s \;|\; s')\,) \quad | \quad [x_c, x_{cc}, x_{id}, x_{amount}]\; bank \bullet charge?\langle x_c, x_{cc}, x_{id}, x_{amount}\rangle.\; x_c \bullet resp!\langle \mathit{chk}(x_{cc}, x_{id}, x_{amount})\rangle$$

μCOWS^m: communication of private names



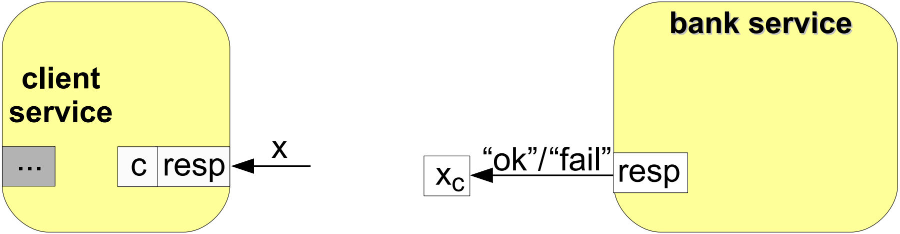
$\equiv$

μCOWS^m: communication of private names



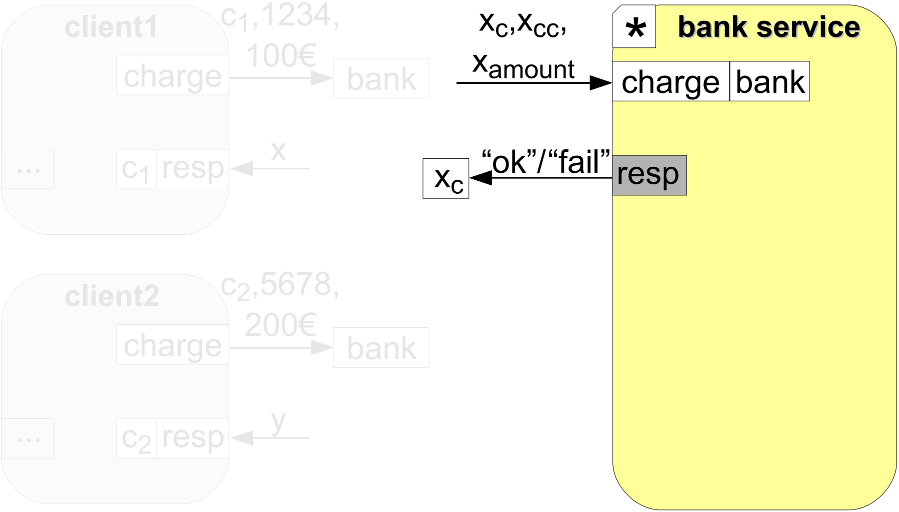
$$[\mathrm{id}, \mathrm{x_c}, \mathrm{x_{cc}}, \mathrm{x_{id}}, \mathrm{x_{amount}}]\left(\begin{pmatrix}\mathrm{bank} \bullet \mathrm{charge}!\langle \mathrm{c}, 1234, \mathrm{id}, 100€\rangle \\ \mid [\mathrm{x}]\,(\mathrm{c} \bullet \mathrm{resp}?\langle \mathrm{x}\rangle.\mathrm{s} \mid \mathrm{s}')\end{pmatrix} \mid \begin{pmatrix}\mathrm{bank} \bullet \mathrm{charge}?\langle \mathrm{x_c}, \mathrm{x_{cc}}, \mathrm{x_{id}}, \mathrm{x_{amount}}\rangle. \\ \mathrm{x_c} \bullet \mathrm{resp}!\langle \mathit{chk}(x_{cc}, x_{id}, x_{amount})\rangle\end{pmatrix}\right)$$

μCOWS^m: communication of private names



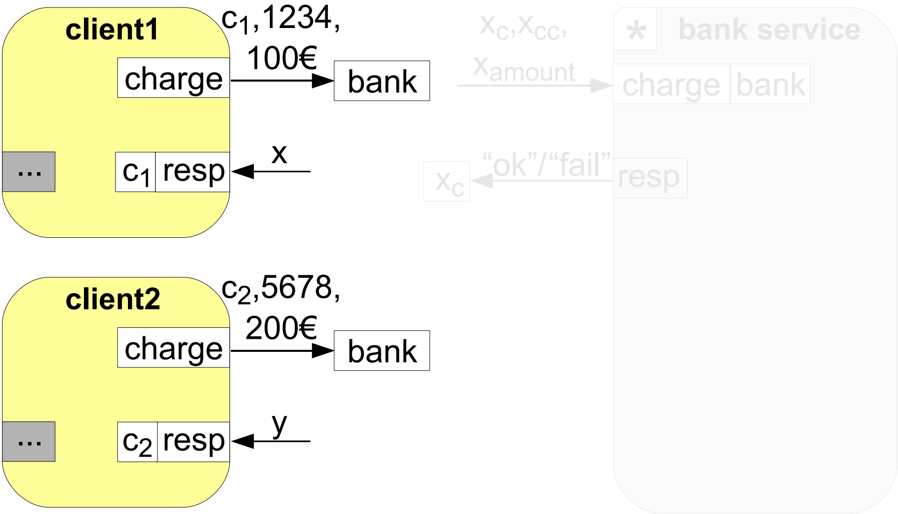
$$[\mathrm{id}]$$
$$(\quad [x]\,(c \bullet resp?\langle x\rangle.s \mid s') \quad\mid\quad c \bullet resp!\langle \mathit{chk}(1234, \mathrm{id}, 100€)\rangle \quad)$$

μCOWS^m: *persistent* bank service example



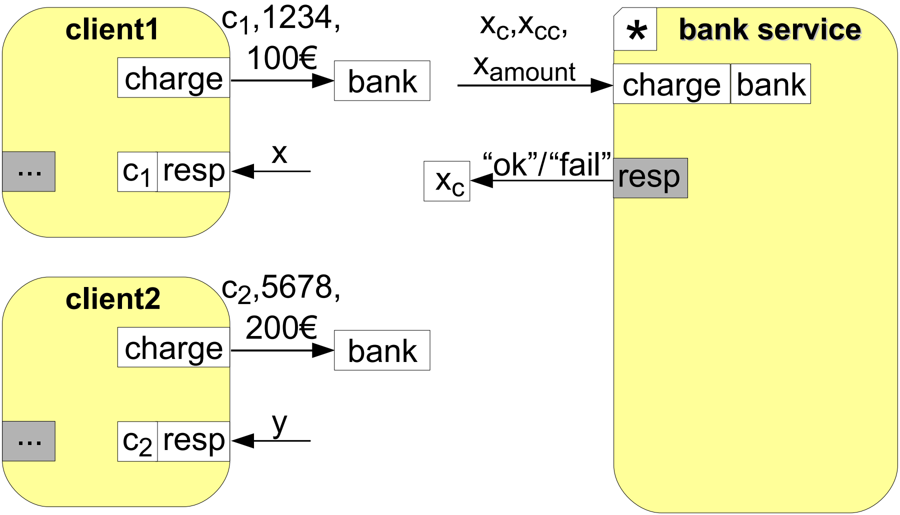
$$* \, [x_c, x_{cc}, x_{amount}] \, \mathrm{bank} \bullet \mathrm{charge}?\langle x_c, x_{cc}, x_{amount}\rangle . x_c \bullet \mathrm{resp}!\langle \mathit{chk}(x_{cc}, x_{amount})\rangle$$

μCOWS^m: *persistent* bank service example

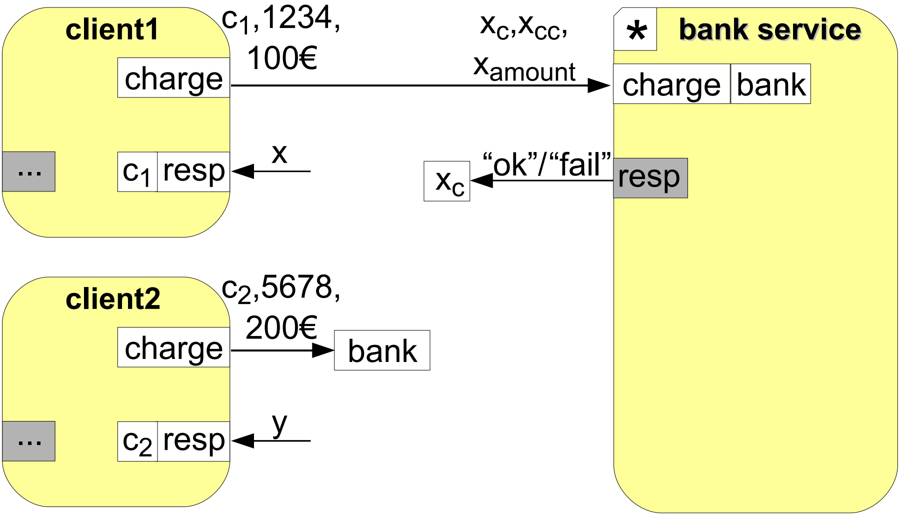


$$\begin{array}{l} \mathsf{bank} \bullet \mathsf{charge}!\langle c_1, 1234, 100€\rangle \mid [x]\, c_1 \bullet \mathsf{resp}?\langle x\rangle.s_1 \\ \mid\ \mathsf{bank} \bullet \mathsf{charge}!\langle c_2, 5678, 200€\rangle \mid [y]\, c_2 \bullet \mathsf{resp}?\langle y\rangle.s_2 \end{array}$$

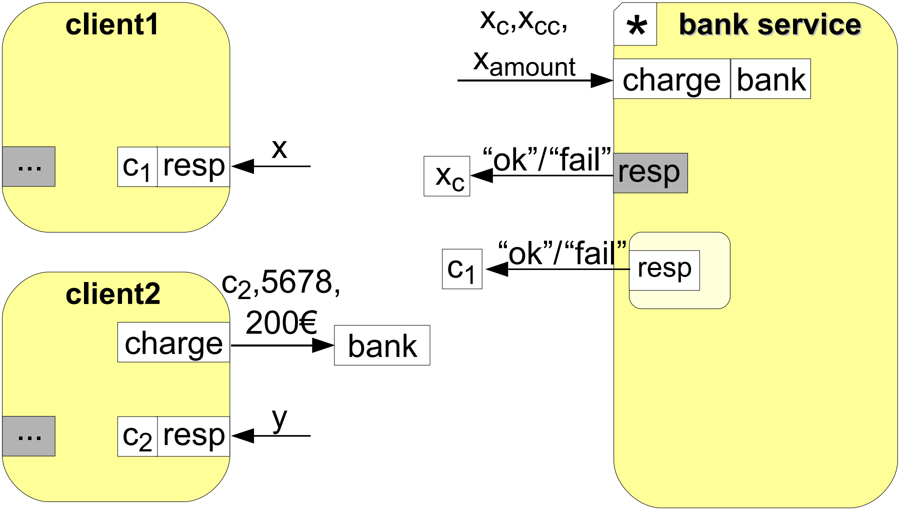
μCOWS^m: *persistent* bank service example



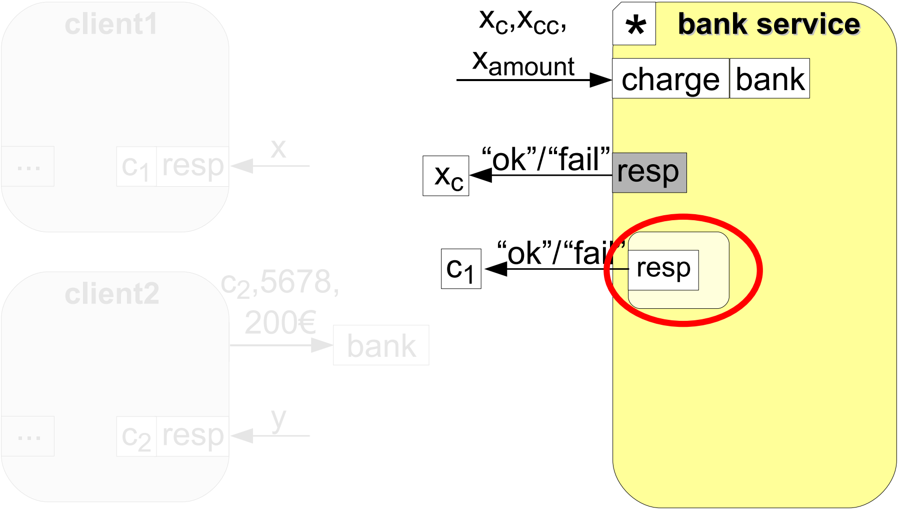
μCOWS^m: *persistent* bank service example



μCOWS^m: *persistent* bank service example



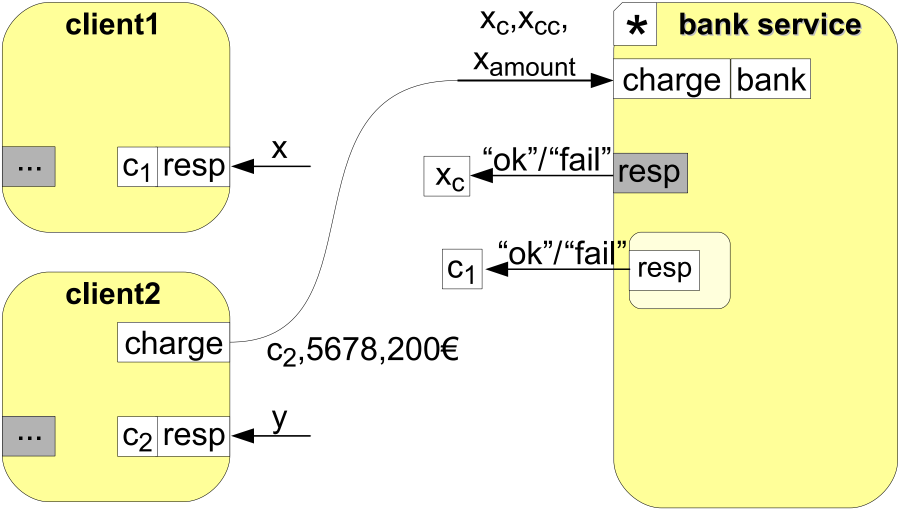
μCOWS^m: *persistent* bank service example



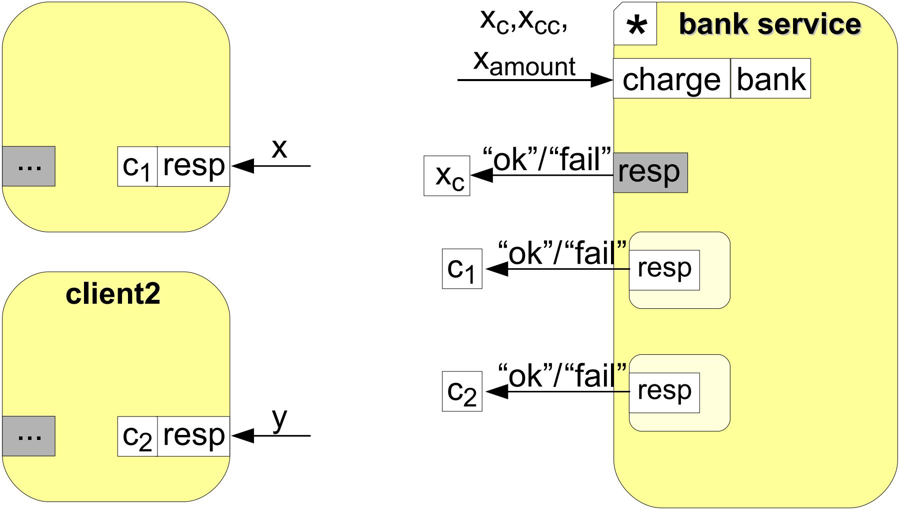
$* \, [x_c, x_{cc}, x_{amount}] \, \mathrm{bank} \bullet \mathrm{charge}?\langle x_c, x_{cc}, x_{amount}\rangle.x_c \bullet \mathrm{resp}!\langle \mathit{chk}(x_{cc}, x_{amount})\rangle$

$\mid \; c_1 \bullet \mathrm{resp}!\langle \mathit{chk}(1234, 100€)\rangle$

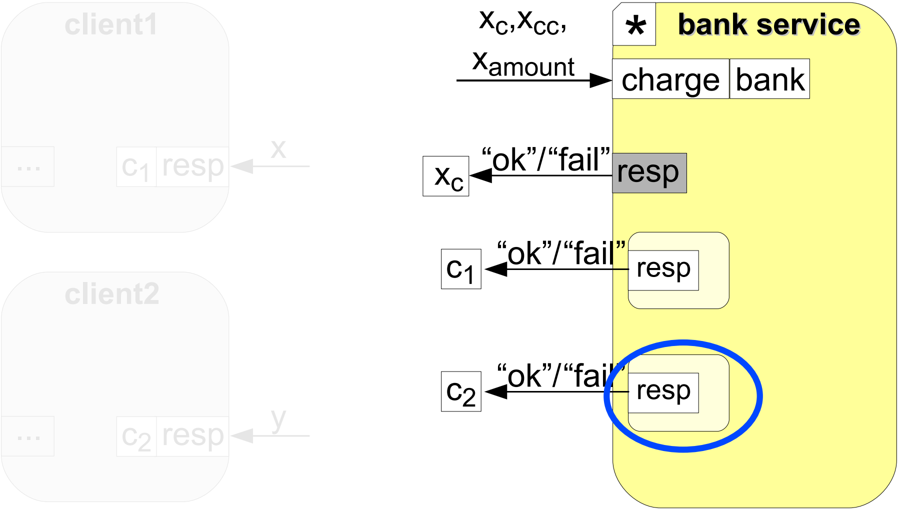
μCOWS^m: *persistent* bank service example



μCOWS^m: *persistent* bank service example



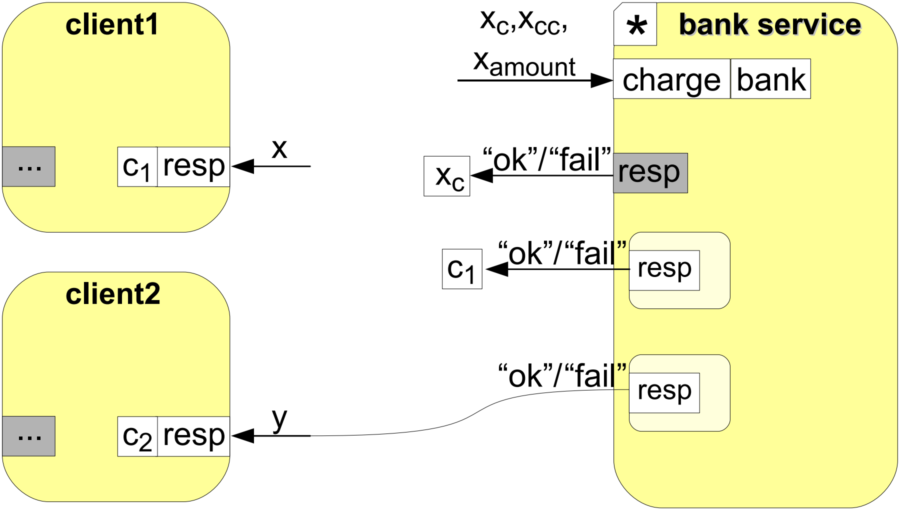
μCOWS^m: *persistent* bank service example



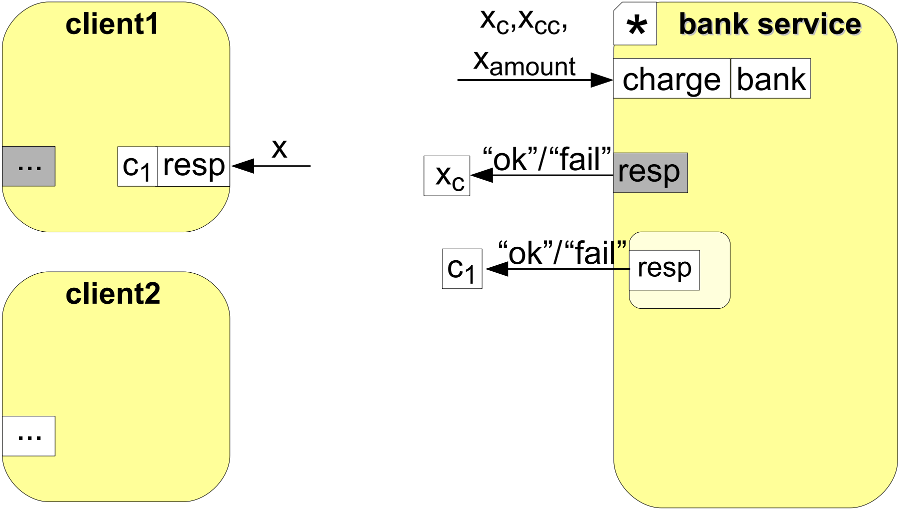
$* \, [\mathrm{x_c}, \mathrm{x_{cc}}, \mathrm{x_{amount}}] \, \mathrm{bank} \bullet \mathrm{charge}?\langle \mathrm{x_c}, \mathrm{x_{cc}}, \mathrm{x_{amount}} \rangle.\mathrm{x_c} \bullet \mathrm{resp}!\langle chk(x_{cc}, x_{amount}) \rangle$

$| \;\; \mathrm{c_1} \bullet \mathrm{resp}!\langle chk(1234, 100€) \rangle \; | \;\; \mathrm{c_2} \bullet \mathrm{resp}!\langle chk(5678, 200€) \rangle$

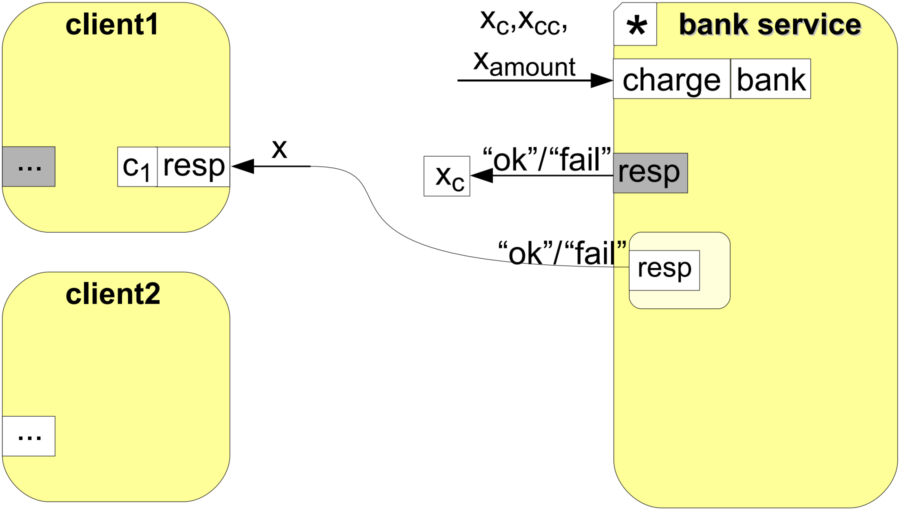
μCOWS^m: *persistent* bank service example



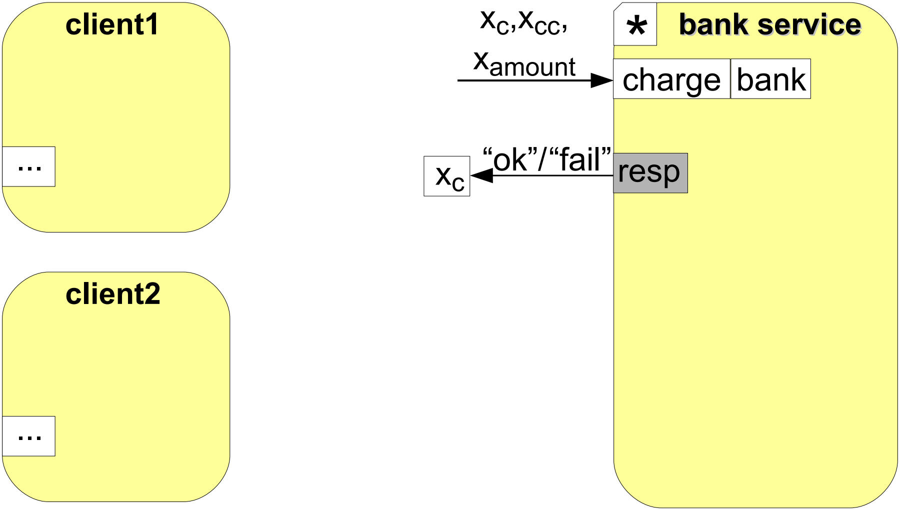
μCOWS^m: *persistent* bank service example



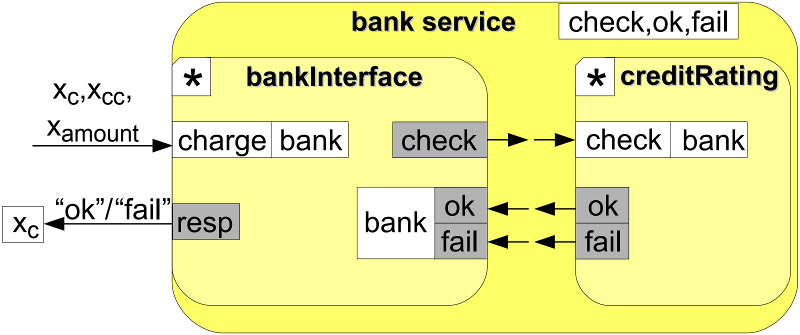
μCOWS^m: *persistent* bank service example



μCOWS^m: *persistent* bank service example

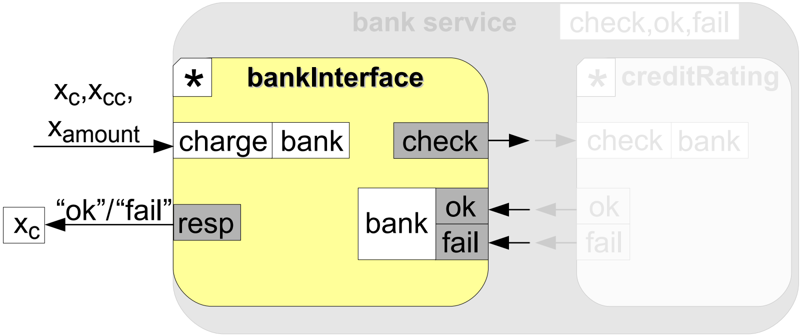


μCOWS^m: *compound* bank service example



$$[check, ok, fail] \,(\, *\, \text{bankInterface} \mid *\, \text{creditRating}\,)$$

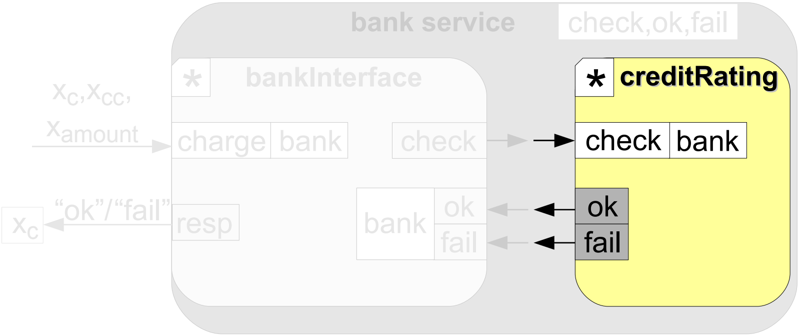
μCOWS^m: *compound* bank service example



$$[\text{check}, \text{ok}, \text{fail}]\,(\,*\,\text{bankInterface} \mid *\,\text{creditRating}\,)$$

$$\begin{array}{lll}
\text{bankInterface} & \triangleq & [x_c, x_{cc}, x_{amount}] \\
& & \text{bank} \bullet \text{charge}?\langle x_c, x_{cc}, x_{amount}\rangle. \\
& & (\,\text{bank} \bullet \text{check}!\langle x_{cc}, x_{amount}\rangle \\
& & \;\mid \text{bank} \bullet \text{ok}?\langle x_{cc}\rangle.\, x_c \bullet \text{resp}!\langle \text{"ok"} \rangle \\
& & \quad + \text{bank} \bullet \text{fail}?\langle x_{cc}\rangle.\, x_c \bullet \text{resp}!\langle \text{"fail"} \rangle\,)
\end{array}$$

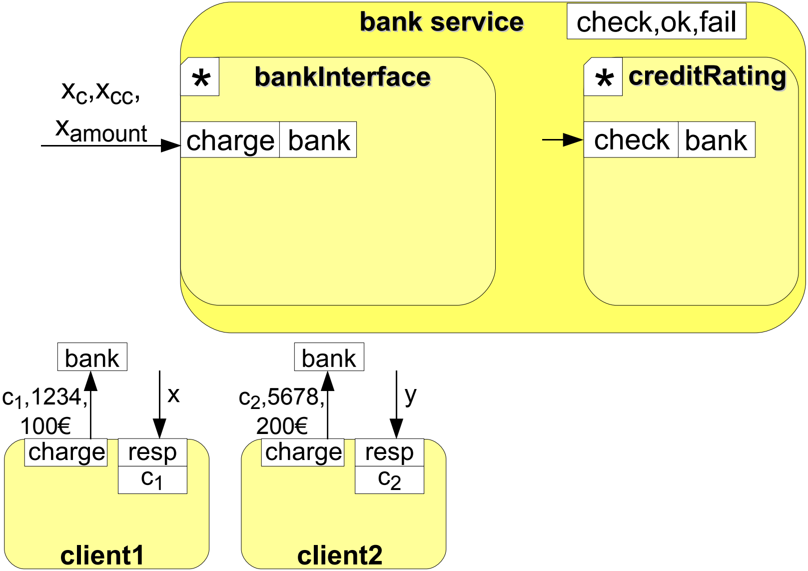
μCOWS^m: *compound* bank service example



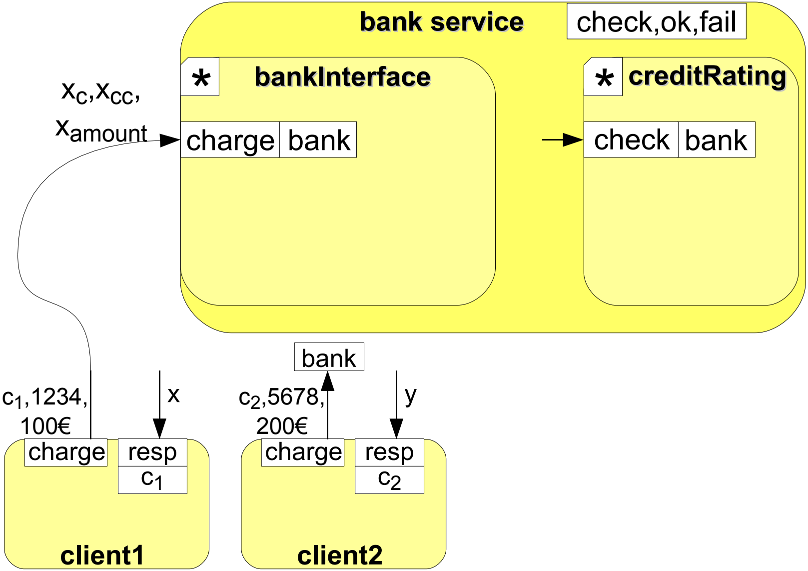
$$[\mathrm{check}, \mathrm{ok}, \mathrm{fail}]\,(\,*\,\mathrm{bankInterface} \mid *\,\mathrm{creditRating}\,)$$

$$\begin{aligned}\mathrm{creditRating} \quad \triangleq \quad & [x_{cc}, x_a] \\ & \mathrm{bank} \bullet \mathrm{check}?\langle x_{cc}, x_a\rangle. \\ & [p, o]\,(\,p \bullet o!\langle\rangle \mid p \bullet o?\langle\rangle.\,\mathrm{bank} \bullet \mathrm{ok}!\langle x_{cc}\rangle \\ & \qquad\qquad\qquad\quad + p \bullet o?\langle\rangle.\,\mathrm{bank} \bullet \mathrm{fail}!\langle x_{cc}\rangle\,)\end{aligned}$$

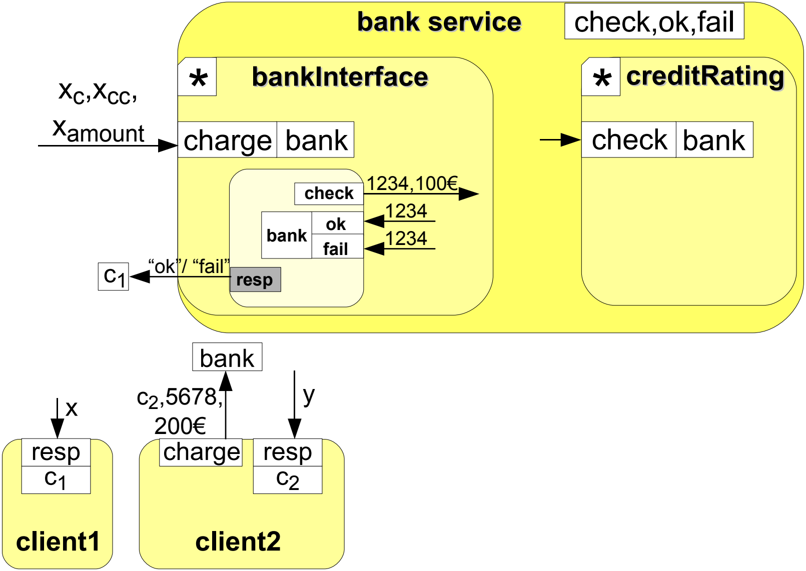
μCOWS^m: *compound* bank service example



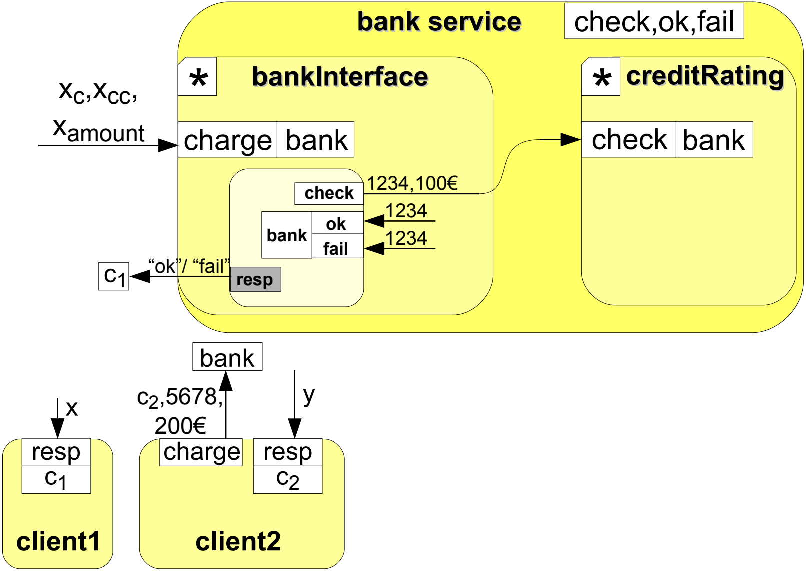
μCOWS^m: *compound* bank service example



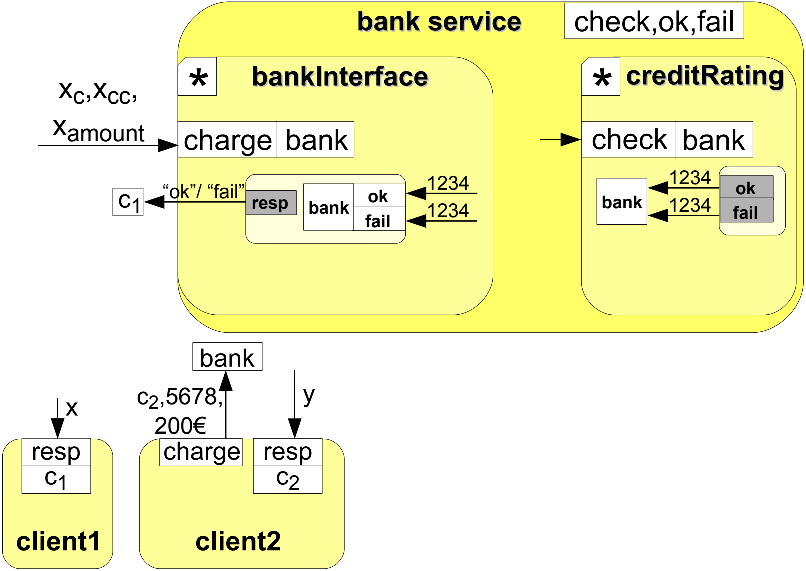
μCOWS^m: *compound* bank service example



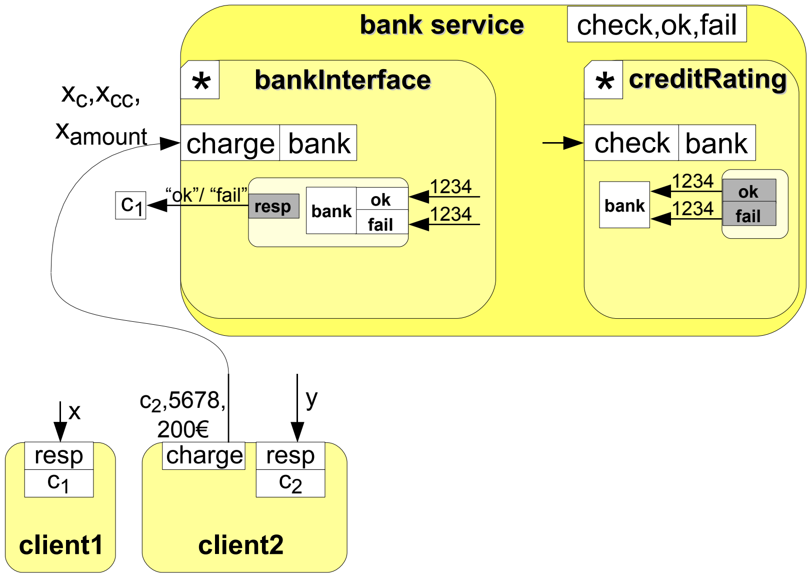
μCOWS^m: *compound* bank service example



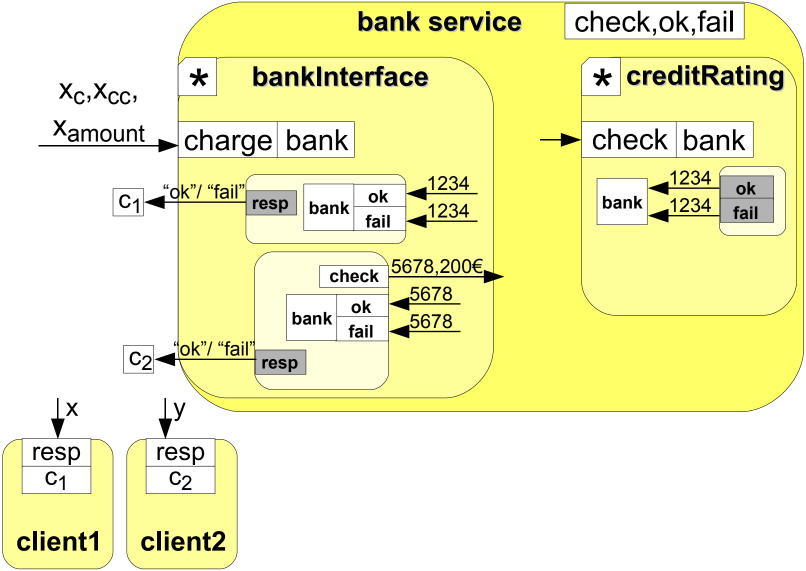
μCOWS^m: *compound* bank service example



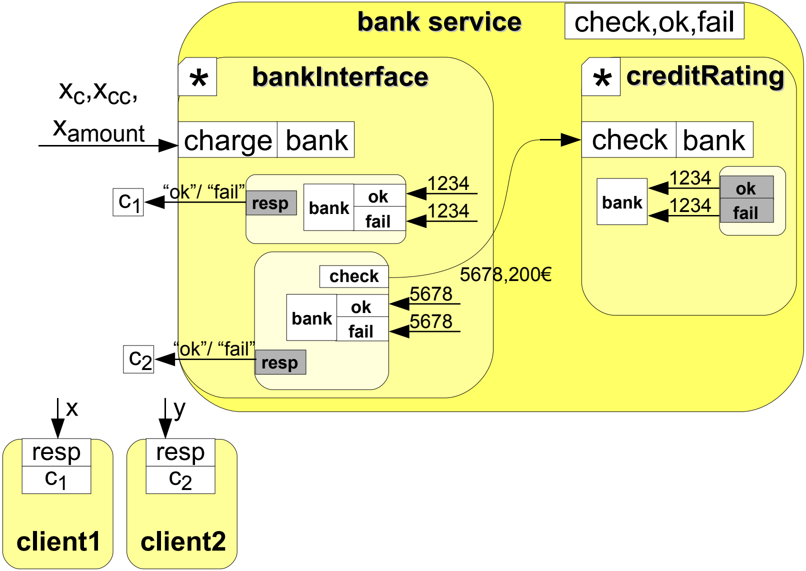
μCOWS^m: *compound* bank service example



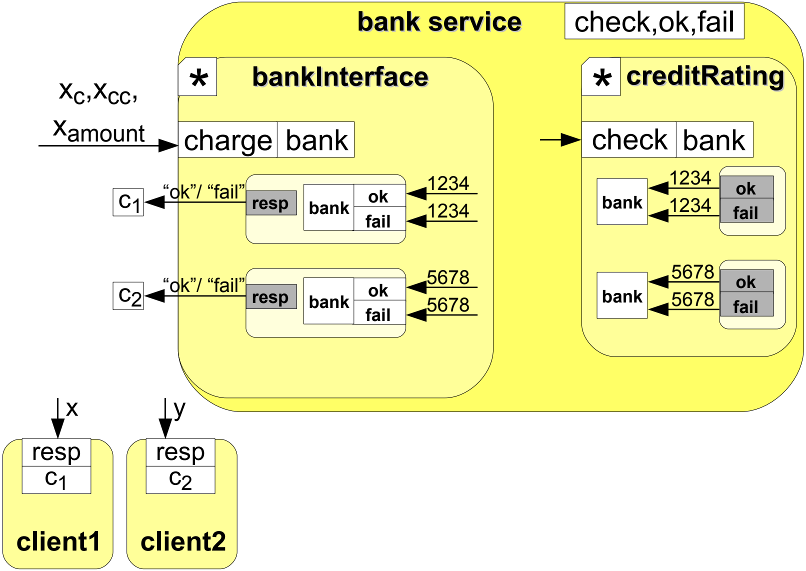
μCOWS^m: *compound* bank service example



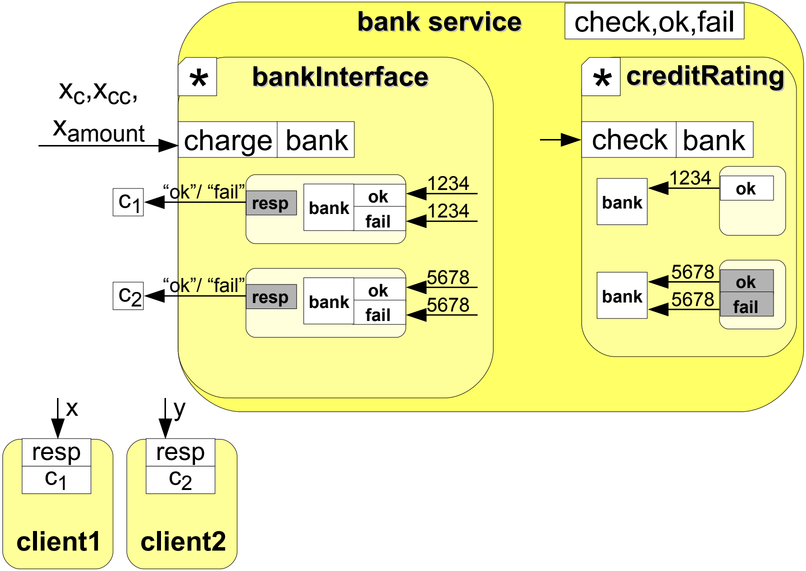
μCOWS^m: *compound* bank service example



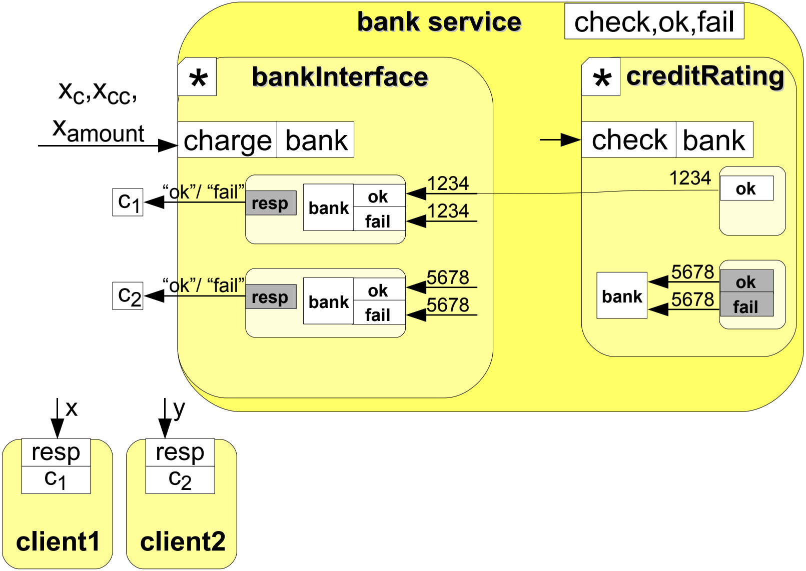
μCOWS^m: *compound* bank service example



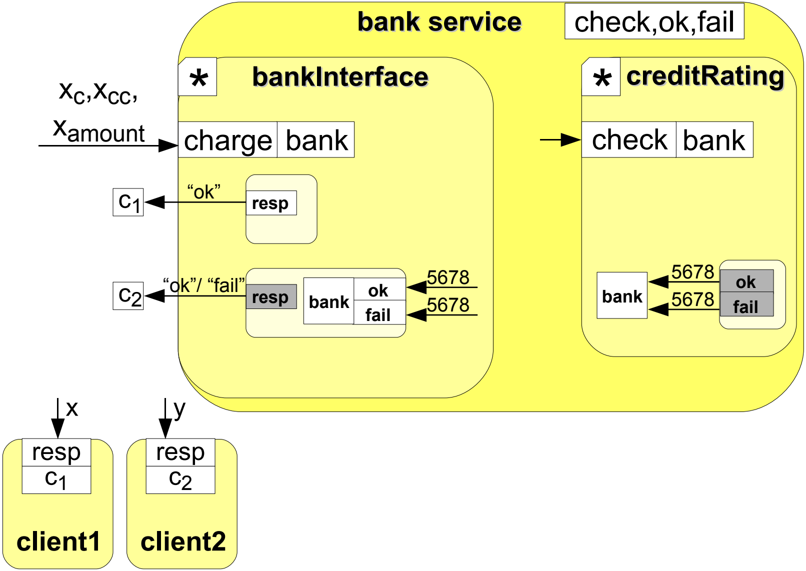
μCOWS^m: *compound* bank service example



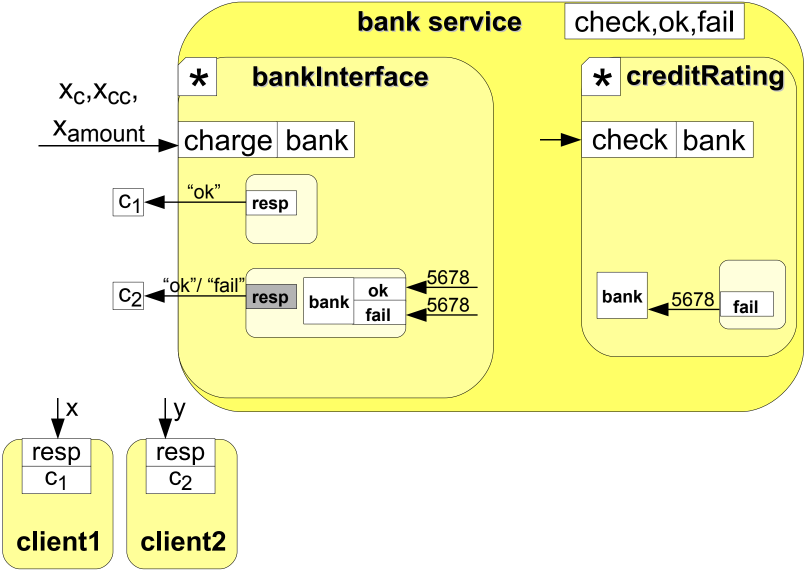
μCOWS^m: *compound* bank service example



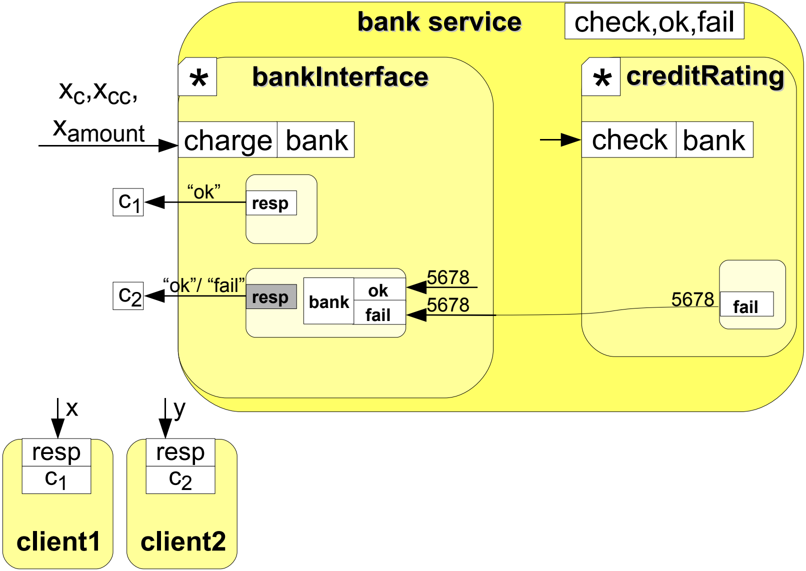
μCOWS^m: *compound* bank service example



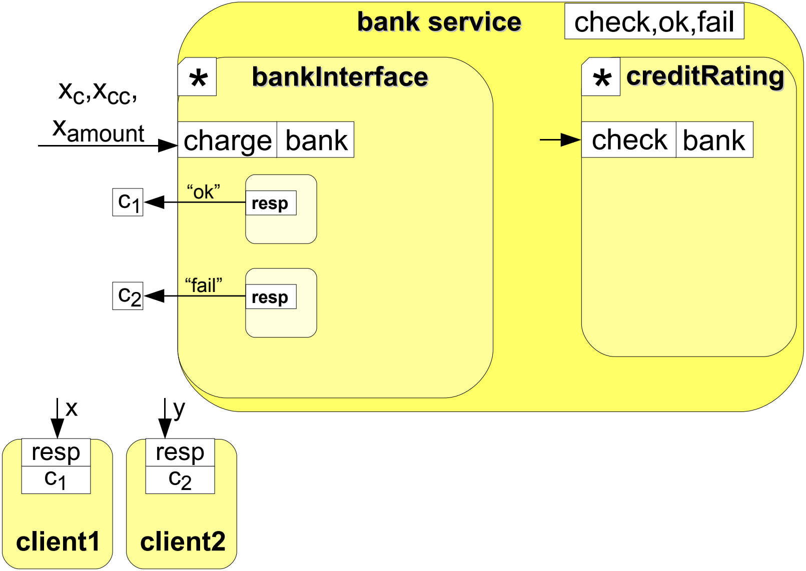
μCOWS^m: *compound* bank service example



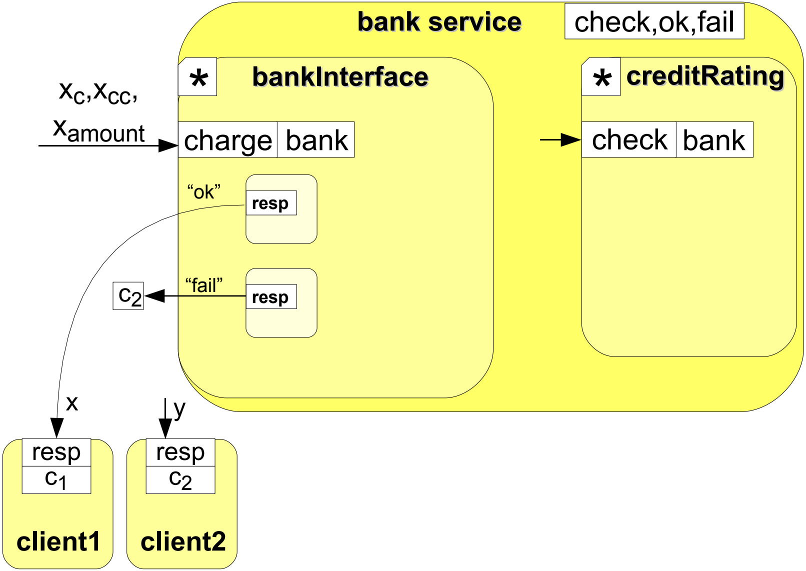
μCOWS^m: *compound* bank service example



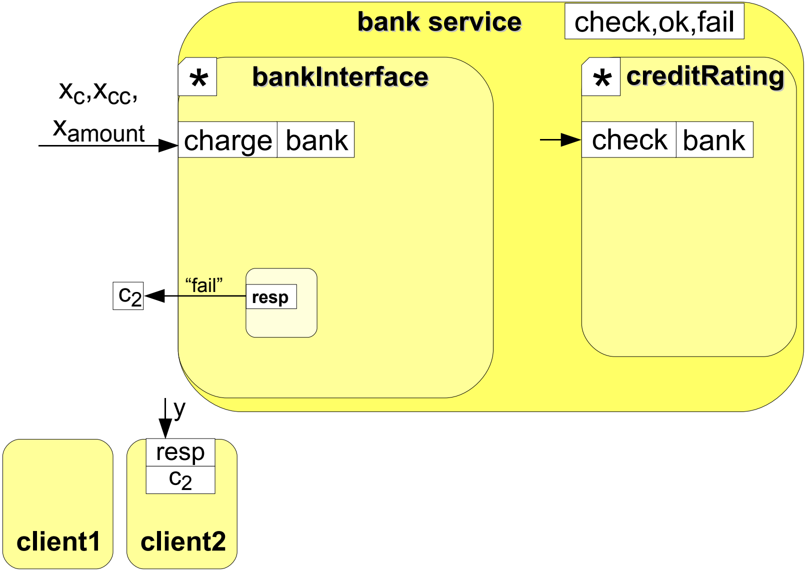
μCOWS^m: *compound* bank service example



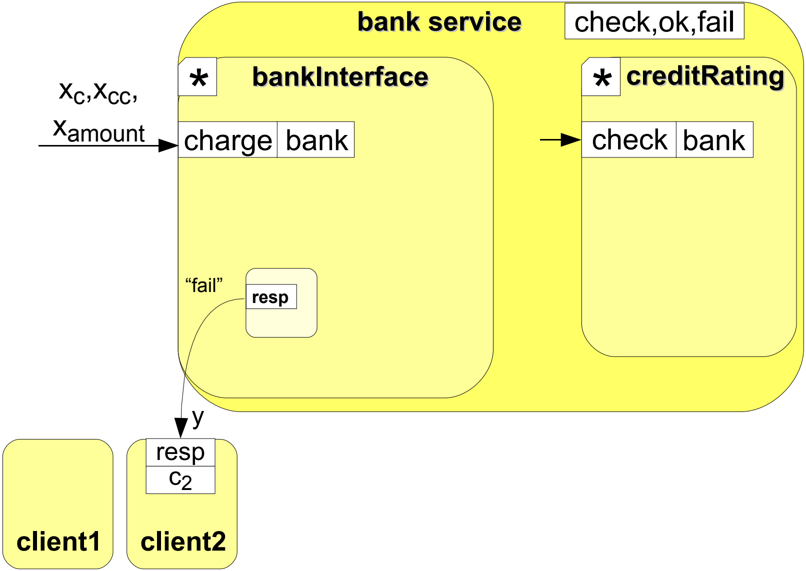
μCOWS^m: *compound* bank service example



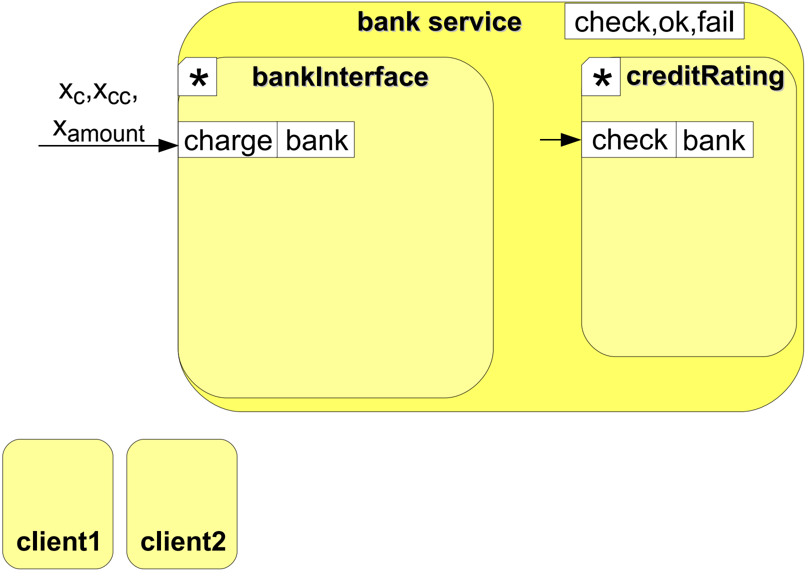
μCOWS^m: *compound* bank service example



μCOWS^m: *compound* bank service example



μCOWS^m: *compound* bank service example



From μCOWS^m to μCOWS

μCOWS^m

From μCOWS^m to μCOWS

μCOWS^m

+

Priority in the parallel composition

From μCOWS^m to μCOWS

μCOWS^m

$+$

Priority in the parallel composition

$=$

μCOWS

μCOWS: why priority in the parallel composition?

1. To deal with *conflicting receives*
   - e.g. in case of multiple start activities
2. Parallel composition with priority can be used (together with pattern-matching) as a *coordination mechanism*
   - e.g. to model default behaviours, transparent session joining, ...

We use a novel combination of *dynamic* priority with *local* pre-emption

dynamic priority: priority values of activities can change as systems evolve

local pre-emption: priorities have a local scope, i.e. prioritised activities can only pre-empt activities in the same scope

μCOWS: why priority in the parallel composition?

1. To deal with *conflicting receives*
   - e.g. in case of multiple start activities
2. Parallel composition with priority can be used (together with pattern-matching) as a *coordination mechanism*
   - e.g. to model default behaviours, transparent session joining, ...

We use a novel combination of *dynamic* priority with *local* pre-emption

dynamic priority: priority values of activities can change as systems evolve

local pre-emption: priorities have a local scope, i.e. prioritised activities can only pre-empt activities in the same scope

μCOWS

Syntax & structural congruence

μCOWS syntax and the set of laws defining its structural congruence coincide with that of μCOWS^m

Labelled transition relation $\xrightarrow{\alpha}$

Label α is now generated by the following grammar:

$$\alpha \quad ::= \quad \mathrm{n} \lhd \bar{v} \quad | \quad \mathrm{n} \rhd \bar{w} \quad | \quad \mathrm{n}\, \sigma\, \ell\, \bar{v}$$

where ℓ is a natural number

μCOWS

Syntax & structural congruence

μCOWS syntax and the set of laws defining its structural congruence coincide with that of μCOWS^m

Labelled transition relation $\xrightarrow{\alpha}$

Label α is now generated by the following grammar:

$$\alpha \quad ::= \quad \mathrm{n} \lhd \bar{v} \quad | \quad \mathrm{n} \rhd \bar{w} \quad | \quad \mathrm{n}\, \sigma\, \ell\, \bar{v}$$

where ℓ is a natural number

μCOWS: Parallel composition with priority

- Communication takes place when two parallel services perform matching receive and invoke activities
- If more then one matching is possible the receive that needs fewer substitutions is selected to progress

$$\frac{s_1 \xrightarrow{\mathrm{n} \triangleright \bar{w}} s_1' \qquad s_2 \xrightarrow{\mathrm{n} \triangleleft \bar{v}} s_2' \qquad \mathcal{M}(\bar{w}, \bar{v}) = \sigma \qquad \mathrm{noConf}(s_1 \mid s_2, \mathrm{n}, \bar{v}, |\sigma|)}{s_1 \mid s_2 \xrightarrow{\mathrm{n}\ \sigma\ |\sigma|\ \bar{v}} s_1' \mid s_2'}$$

Conflicting receives predicate

$\mathrm{noConf}(s, \mathrm{n}, \bar{v}, \ell)$ checks existence of potential communication conflicts, i.e. the ability of s of performing a receive activity matching $\bar{v}$ over the endpoint n that generates a substitution with fewer pairs than ℓ

μCOWS: Parallel composition with priority

- Communication takes place when two parallel services perform matching receive and invoke activities
- If more then one matching is possible the receive that needs fewer substitutions is selected to progress

$$\frac{s_1 \xrightarrow{\mathrm{n} \triangleright \bar{w}} s_1' \qquad s_2 \xrightarrow{\mathrm{n} \triangleleft \bar{v}} s_2' \qquad \mathcal{M}(\bar{w}, \bar{v}) = \sigma \qquad \mathrm{noConf}(s_1 \mid s_2, \mathrm{n}, \bar{v}, |\sigma|)}{s_1 \mid s_2 \xrightarrow{\mathrm{n}\ \sigma\ |\sigma|\ \bar{v}} s_1' \mid s_2'}$$

Conflicting receives predicate

$\mathrm{noConf}(s, \mathrm{n}, \bar{v}, \ell)$ checks existence of potential communication conflicts, i.e. the ability of s of performing a receive activity matching $\bar{v}$ over the endpoint n that generates a substitution with fewer pairs than ℓ

μCOWS: Parallel composition with priority

- Communication takes place when two parallel services perform matching receive and invoke activities
- If more then one matching is possible the receive that needs fewer substitutions is selected to progress

$$\frac{s_1 \xrightarrow{\mathrm{n} \triangleright \bar{w}} s_1' \qquad s_2 \xrightarrow{\mathrm{n} \triangleleft \bar{v}} s_2' \qquad \mathcal{M}(\bar{w}, \bar{v}) = \sigma \qquad \mathrm{noConf}(s_1 \mid s_2, \mathrm{n}, \bar{v}, |\sigma|)}{s_1 \mid s_2 \xrightarrow{\mathrm{n}\ \sigma\ |\sigma|\ \bar{v}} s_1' \mid s_2'}$$

Conflicting receives predicate

$\mathrm{noConf}(s, \mathrm{n}, \bar{v}, \ell)$ checks existence of potential communication conflicts, i.e. the ability of s of performing a receive activity matching $\bar{v}$ over the endpoint n that generates a substitution with fewer pairs than ℓ

μCOWS: Parallel composition with priority

- Communication takes place when two parallel services perform matching receive and invoke activities
- If more then one matching is possible the receive that needs fewer substitutions is selected to progress

$$\frac{s_1 \xrightarrow{\mathrm{n} \rhd \bar{w}} s_1' \qquad s_2 \xrightarrow{\mathrm{n} \lhd \bar{v}} s_2' \qquad \mathcal{M}(\bar{w}, \bar{v}) = \sigma \qquad \mathrm{noConf}(s_1 \mid s_2, \mathrm{n}, \bar{v}, |\sigma|)}{s_1 \mid s_2 \xrightarrow{\mathrm{n}\,\sigma\,|\sigma|\,\bar{v}} s_1' \mid s_2'}$$

Conflicting receives predicate (inductive definition, part 1/2)

$$\mathrm{noConf}(\mathbf{kill}(k), \mathrm{n}, \bar{v}, \ell) = \mathrm{noConf}(\mathrm{u}!\bar{\epsilon}, \mathrm{n}, \bar{v}, \ell) = \textbf{true}$$

$$\mathrm{noConf}(\textstyle\sum_{i=1}^{r} \mathrm{n}_i?\bar{w}_i.s_i, \mathrm{n}, \bar{v}, \ell) = \begin{cases} \textbf{false} & \text{if } \exists\, i \,.\, \mathrm{n}_i = \mathrm{n} \wedge |\mathcal{M}(\bar{w}_i, \bar{v})| < \ell \\ \textbf{true} & \text{otherwise} \end{cases}$$

μCOWS: Parallel composition with priority

- Communication takes place when two parallel services perform matching receive and invoke activities
- If more then one matching is possible the receive that needs fewer substitutions is selected to progress

$$\frac{s_1 \xrightarrow{\mathrm{n} \rhd \bar{w}} s_1' \qquad s_2 \xrightarrow{\mathrm{n} \lhd \bar{v}} s_2' \qquad \mathcal{M}(\bar{w}, \bar{v}) = \sigma \qquad \mathrm{noConf}(s_1 \mid s_2, \mathrm{n}, \bar{v}, |\sigma|)}{s_1 \mid s_2 \xrightarrow{\mathrm{n}\,\sigma\,|\sigma|\,\bar{v}} s_1' \mid s_2'}$$

Conflicting receives predicate (inductive definition, part 2/2)

$$\mathrm{noConf}(s \mid s', \mathrm{n}, \bar{v}, \ell) = \mathrm{noConf}(s, \mathrm{n}, \bar{v}, \ell) \wedge \mathrm{noConf}(s', \mathrm{n}, \bar{v}, \ell)$$

$$\mathrm{noConf}([u]\, s, \mathrm{n}, \bar{v}, \ell) = \begin{cases} \mathrm{noConf}(s, \mathrm{n}, \bar{v}, \ell) & \text{if } u \notin \mathrm{n} \\ \textbf{true} & \text{otherwise} \end{cases}$$

$$\mathrm{noConf}(\{|s|\}, \mathrm{n}, \bar{v}, \ell) = \mathrm{noConf}(*\, s, \mathrm{n}, \bar{v}, \ell) = \mathrm{noConf}(s, \mathrm{n}, \bar{v}, \ell)$$

μCOWS: Parallel composition with priority

- Execution of parallel services is interleaved, when no communication is involved:

$$\frac{s_1 \xrightarrow{\alpha} s_1' \qquad \alpha \neq \mathrm{n}\,\sigma\,\ell\,\bar{v}}{s_1 \mid s_2 \xrightarrow{\alpha} s_1' \mid s_2}$$

- In case of communications, the receive activity with greater priority progresses:

$$\frac{s_1 \xrightarrow{\mathrm{n}\,\sigma\,\ell\,\bar{v}} s_1' \qquad \mathrm{noConf}(s_2, \mathrm{n}, \bar{v}, \ell)}{s_1 \mid s_2 \xrightarrow{\mathrm{n}\,\sigma\,\ell\,\bar{v}} s_1' \mid s_2}$$

μCOWS: Parallel composition with priority

- Execution of parallel services is interleaved, when no communication is involved:

$$\frac{s_1 \xrightarrow{\alpha} s_1' \qquad \alpha \neq \mathrm{n}\,\sigma\,\ell\,\bar{v}}{s_1 \mid s_2 \xrightarrow{\alpha} s_1' \mid s_2}$$

- In case of communications, the receive activity with greater priority progresses:

$$\frac{s_1 \xrightarrow{\mathrm{n}\,\sigma\,\ell\,\bar{v}} s_1' \qquad \mathrm{noConf}(s_2, \mathrm{n}, \bar{v}, \ell)}{s_1 \mid s_2 \xrightarrow{\mathrm{n}\,\sigma\,\ell\,\bar{v}} s_1' \mid s_2}$$

μCOWS: Parallel composition with priority

- Execution of parallel services is interleaved, when no communication is involved:

$$\frac{s_1 \xrightarrow{\alpha} s_1' \qquad \alpha \neq \mathtt{n}\,\sigma\,\ell\,\bar{v}}{s_1 \mid s_2 \xrightarrow{\alpha} s_1' \mid s_2}$$

- In case of communications, the receive activity with greater priority progresses:

$$\frac{s_1 \xrightarrow{\mathtt{n}\,\sigma\,\ell\,\bar{v}} s_1' \qquad \mathrm{noConf}(s_2, \mathtt{n}, \bar{v}, \ell)}{s_1 \mid s_2 \xrightarrow{\mathtt{n}\,\sigma\,\ell\,\bar{v}} s_1' \mid s_2}$$

μCOWS: Delimitation

- Rules for delimitation are tailored to deal with labels $\mathrm{n}\,\sigma\,\ell\,\bar{v}$

$$\frac{s \xrightarrow{\mathrm{n}\ \sigma \uplus \{x \mapsto v\}\ \ell\ \bar{v}} s'}{[x]\, s \xrightarrow{\mathrm{n}\ \sigma\ \ell\ \bar{v}} s' \cdot \{x \mapsto v\}} \qquad \frac{s \xrightarrow{\alpha} s' \quad u \notin \mathrm{u}(\alpha)}{[u]\, s \xrightarrow{\alpha} [u]\, s'}$$

where

- $\mathrm{u}(\alpha)$ is extended with $\mathrm{u}(\mathrm{n}\,\sigma\,\ell\,\bar{v}) = \mathrm{u}(\sigma)$

μCOWS: Delimitation

- Rules for delimitation are tailored to deal with labels $\mathrm{n}\,\sigma\,\ell\,\bar{v}$

$$\frac{s \xrightarrow{\mathrm{n}\ \sigma \uplus \{x \mapsto v\}\ \ell\ \bar{v}} s'}{[x]\,s \xrightarrow{\mathrm{n}\ \sigma\ \ell\ \bar{v}} s' \cdot \{x \mapsto v\}} \qquad \frac{s \xrightarrow{\alpha} s' \quad u \notin \mathrm{u}(\alpha)}{[u]\,s \xrightarrow{\alpha} [u]\,s'}$$

  where

  - $\mathrm{u}(\alpha)$ is extended with $\mathrm{u}(\mathrm{n}\,\sigma\,\ell\,\bar{v}) = \mathrm{u}(\sigma)$

μCOWS operational semantics

Labelled transition rules

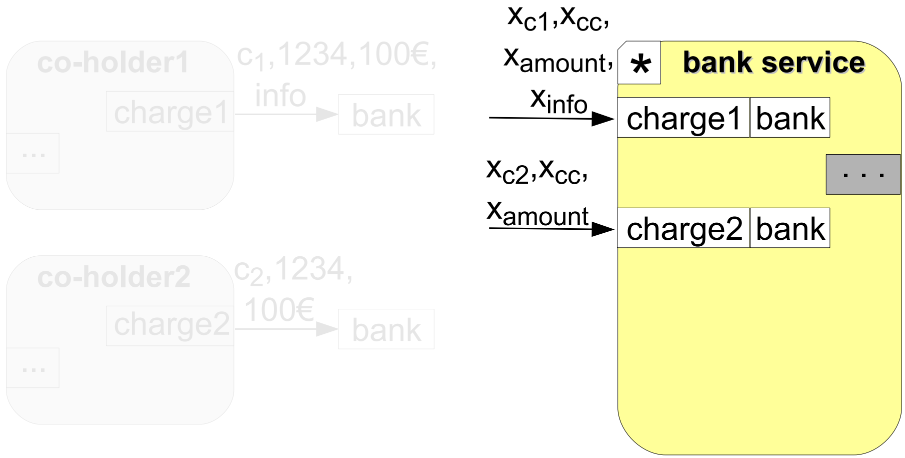
$$\frac{[\![\bar{\epsilon}]\!] = \bar{v}}{\mathrm{n}!\bar{\epsilon} \xrightarrow{\mathrm{n} \lhd \bar{v}} \mathbf{0}} \qquad \frac{1 \leq j \leq r}{\sum_{i=1}^{r} \mathrm{n}_i?\bar{w}_i.s_i \xrightarrow{\mathrm{n}_j \rhd \bar{w}_j} s_j} \qquad \frac{s \xrightarrow{\alpha} s' \quad u \notin \mathrm{u}(\alpha)}{[u]\, s \xrightarrow{\alpha} [u]\, s'} \qquad \frac{s \equiv \xrightarrow{\alpha} \equiv s'}{s \xrightarrow{\alpha} s'}$$

$$\frac{s_1 \xrightarrow{\mathrm{n} \rhd \bar{w}} s_1' \quad s_2 \xrightarrow{\mathrm{n} \lhd \bar{v}} s_2' \quad \mathcal{M}(\bar{w}, \bar{v}) = \sigma \quad \mathrm{noConf}(s_1 \mid s_2, \mathrm{n}, \bar{v}, |\sigma|)}{s_1 \mid s_2 \xrightarrow{\mathrm{n}\, \sigma\, |\sigma|\, \bar{v}} s_1' \mid s_2'}$$

$$\frac{s_1 \xrightarrow{\alpha} s_1' \qquad \alpha \neq \mathrm{n}\, \sigma\, \ell\, \bar{v}}{s_1 \mid s_2 \xrightarrow{\alpha} s_1' \mid s_2} \qquad \frac{s_1 \xrightarrow{\mathrm{n}\, \sigma\, \ell\, \bar{v}} s_1' \qquad \mathrm{noConf}(s_2, \mathrm{n}, \bar{v}, \ell)}{s_1 \mid s_2 \xrightarrow{\mathrm{n}\, \sigma\, \ell\, \bar{v}} s_1' \mid s_2}$$

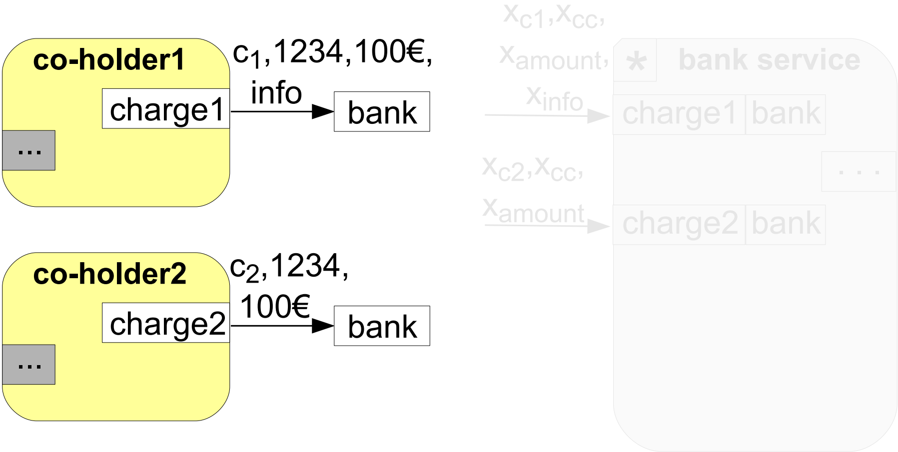
$$\frac{s \xrightarrow{\mathrm{n}\, \sigma \uplus \{x \mapsto v\}\, \ell\, \bar{v}} s'}{[x]\, s \xrightarrow{\mathrm{n}\, \sigma\, \ell\, \bar{v}} s' \cdot \{x \mapsto v\}}$$

μCOWS: *joint account* service example



$$
\begin{aligned}
* \,[x_{c1}, x_{c2}, x_{cc}, x_{amount}, x_{info}]\; (\, & \mathrm{bank} \bullet \mathrm{charge1}?\langle x_{c1}, x_{cc}, x_{amount}, x_{info}\rangle.s_1 \\
\mid\; & \mathrm{bank} \bullet \mathrm{charge2}?\langle x_{c2}, x_{cc}, x_{amount}\rangle.s_2\,) \\
\mid\; (\, \mathrm{bank} \bullet \mathrm{charge1}!\langle c_1, 1234, 100€, \mathrm{info}\rangle \mid s_1' \,) & \\
\mid\; (\, \mathrm{bank} \bullet \mathrm{charge2}!\langle c_2, 1234, 100€\rangle \mid s_2' \,) &
\end{aligned}
$$

μCOWS: *joint account* service example

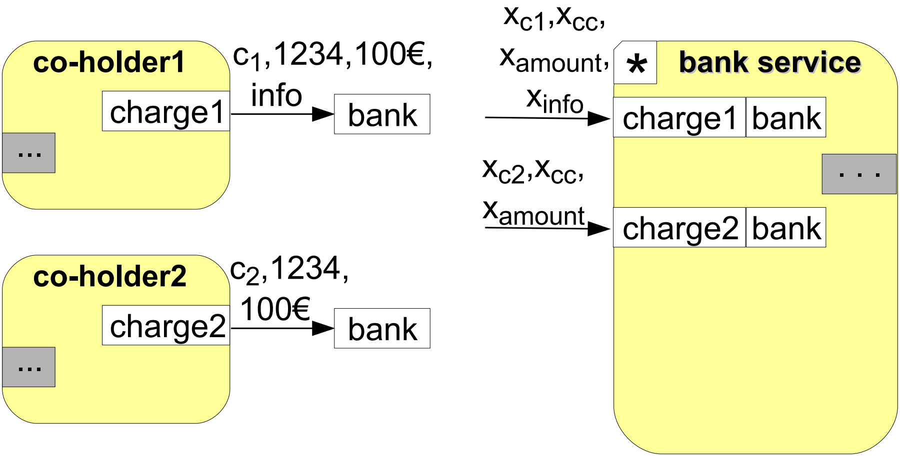


$$* \; [x_{c1}, x_{c2}, x_{cc}, x_{amount}, x_{info}] \, (\mathrm{bank} \bullet \mathrm{charge1}?\langle x_{c1}, x_{cc}, x_{amount}, x_{info} \rangle . s_1 \; | \; \mathrm{bank} \bullet \mathrm{charge2}?\langle x_{c2}, x_{cc}, x_{amount} \rangle . s_2 \,)$$

$$| \; (\mathrm{bank} \bullet \mathrm{charge1}!\langle c_1, 1234, 100€, \mathrm{info} \rangle \; | \; s'_1 \,)$$

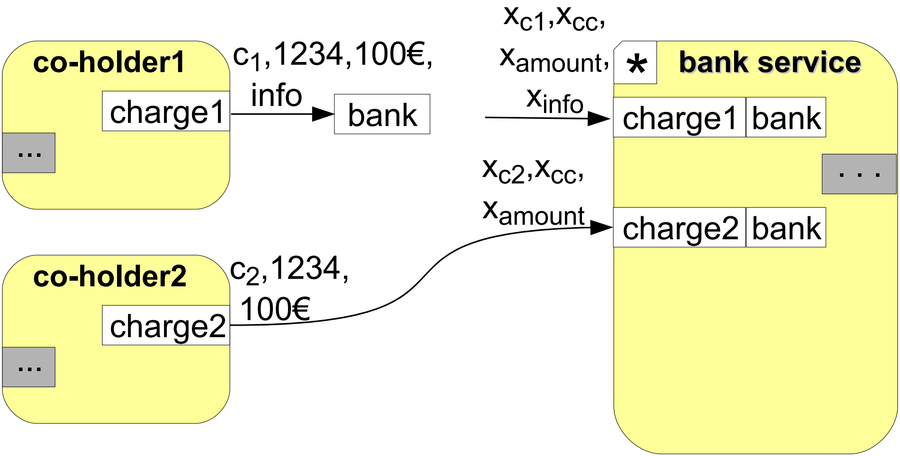
$$| \; (\mathrm{bank} \bullet \mathrm{charge2}!\langle c_2, 1234, 100€ \rangle \; | \; s'_2 \,)$$

μCOWS: *joint account* service example



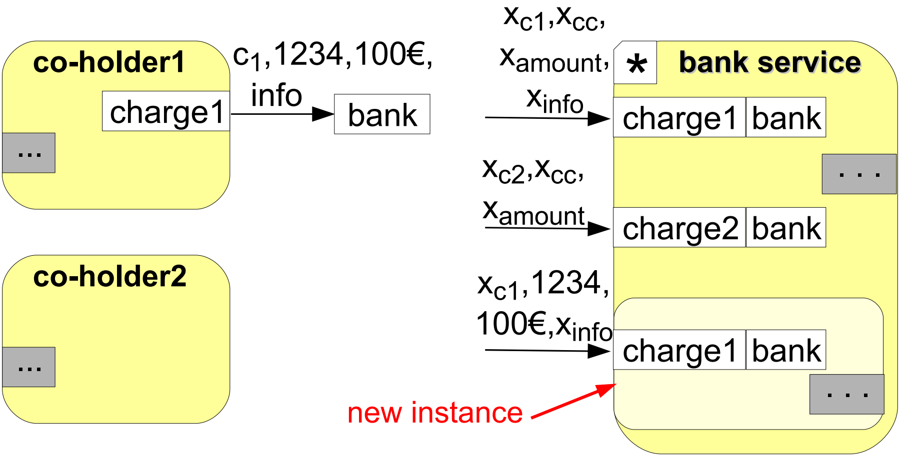
$$
\begin{array}{l}
* \, [\mathrm{x}_{c1}, \mathrm{x}_{c2}, \mathrm{x}_{cc}, \mathrm{x}_{amount}, \mathrm{x}_{info}] \, (\, \mathrm{bank} \bullet \mathrm{charge1} ? \langle \mathrm{x}_{c1}, \mathrm{x}_{cc}, \mathrm{x}_{amount}, \mathrm{x}_{info} \rangle . s_1 \\
\qquad\qquad\qquad\qquad\qquad\quad \mid \, \mathrm{bank} \bullet \mathrm{charge2} ? \langle \mathrm{x}_{c2}, \mathrm{x}_{cc}, \mathrm{x}_{amount} \rangle . s_2 \,) \\
\mid \, (\, \mathrm{bank} \bullet \mathrm{charge1} ! \langle \mathrm{c}_1, 1234, 100€, \mathrm{info} \rangle \mid s_1' \,) \\
\mid \, (\, \mathrm{bank} \bullet \mathrm{charge2} ! \langle \mathrm{c}_2, 1234, 100€ \rangle \mid s_2' \,)
\end{array}
$$

μCOWS: *joint account* service example



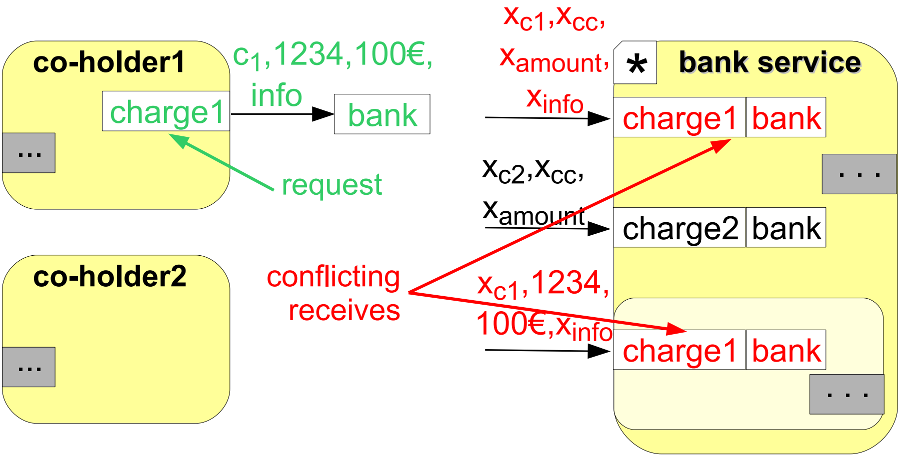
$$
\begin{array}{l}
* \, [\mathrm{x_{c1}}, \mathrm{x_{c2}}, \mathrm{x_{cc}}, \mathrm{x_{amount}}, \mathrm{x_{info}}] \, (\, \mathrm{bank} \bullet \mathrm{charge1} ? \langle \mathrm{x_{c1}}, \mathrm{x_{cc}}, \mathrm{x_{amount}}, \mathrm{x_{info}} \rangle . s_1 \\
\qquad\qquad\qquad\qquad\qquad \mid \, \mathrm{bank} \bullet \mathrm{charge2} ? \langle \mathrm{x_{c2}}, \mathrm{x_{cc}}, \mathrm{x_{amount}} \rangle . s_2 \,) \\
\mid \; (\, \mathrm{bank} \bullet \mathrm{charge1} ! \langle \mathrm{c_1}, 1234, 100€, \mathrm{info} \rangle \mid s_1' \,) \\
\mid \; (\, \mathrm{bank} \bullet \mathrm{charge2} ! \langle \mathrm{c_2}, 1234, 100€ \rangle \mid s_2' \,)
\end{array}
$$

μCOWS: *joint account* service example



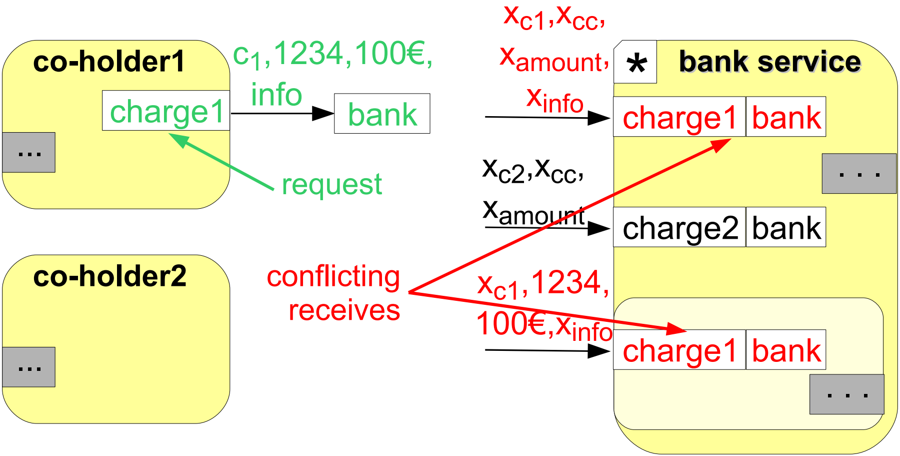
$$
\begin{array}{l}
* \, [x_{c1}, x_{c2}, x_{cc}, x_{amount}, x_{info}] \, (\mathrm{bank} \bullet \mathrm{charge1}?\langle x_{c1}, x_{cc}, x_{amount}, x_{info} \rangle . s_1 \\
\qquad\qquad\qquad\qquad \mid \; \mathrm{bank} \bullet \mathrm{charge2}?\langle x_{c2}, x_{cc}, x_{amount} \rangle . s_2 \,) \\
\mid \; (\mathrm{bank} \bullet \mathrm{charge1}?\langle x_{c1}, 1234, 100€, x_{info} \rangle . s_1 \; \mid \; s_2 \,) \cdot \{ \cdots \mapsto \cdots \} \\
\mid \; (\mathrm{bank} \bullet \mathrm{charge1}!\langle c_1, 1234, 100€, \mathrm{info} \rangle \; \mid \; s'_1 \,) \; \mid \; (\, s'_2 \,)
\end{array}
$$

μCOWS: *joint account* service example



$$
\begin{array}{l}
* \, [x_{c1}, x_{c2}, x_{cc}, x_{amount}, x_{info}] \, (\, bank \bullet charge1?\langle x_{c1}, x_{cc}, x_{amount}, x_{info} \rangle . s_1 \\
\qquad\qquad\qquad\qquad\qquad \mid \; bank \bullet charge2?\langle x_{c2}, x_{cc}, x_{amount} \rangle . s_2 \,) \\
\mid \; (\, bank \bullet charge1?\langle x_{c1}, 1234, 100€, x_{info} \rangle . s_1 \; \mid \; s_2 \,) \cdot \{ \cdots \mapsto \cdots \} \\
\mid \; (\, bank \bullet charge1!\langle c_1, 1234, 100€, info \rangle \; \mid \; s'_1 \,) \; \mid \; (\, s'_2 \,)
\end{array}
$$

μCOWS: *joint account* service example

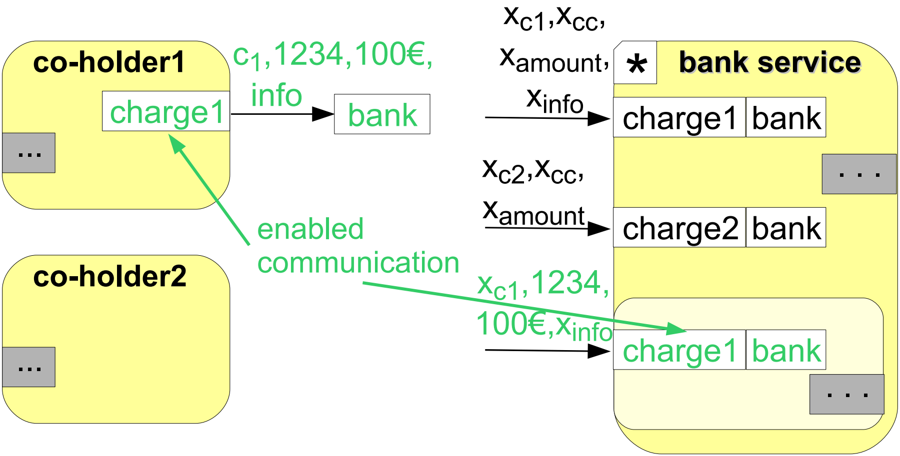


Multiple start activities

The service can receive multiple messages in a statically unpredictable order s.t.

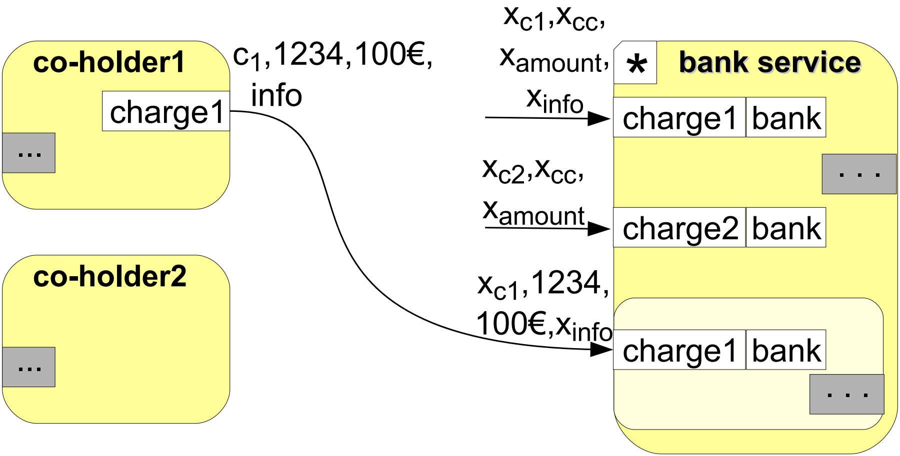
- the first incoming message triggers creation of a service instance
- subsequent messages are delivered to the created instance

μCOWS: *joint account* service example



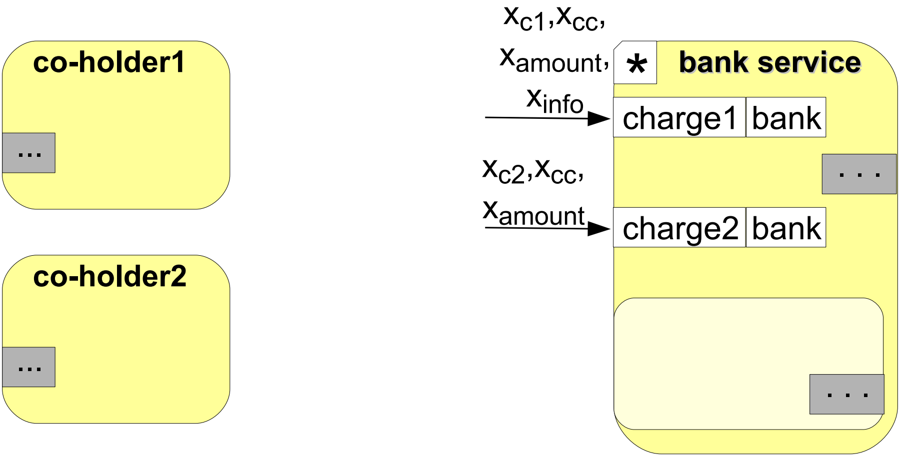
$$
\begin{array}{l}
* \, [x_{c1}, x_{c2}, x_{cc}, x_{amount}, x_{info}] \, (\, \mathrm{bank} \bullet \mathrm{charge1}?\langle x_{c1}, x_{cc}, x_{amount}, x_{info}\rangle.s_1 \\
\qquad\qquad\qquad\qquad\qquad \mid \; \mathrm{bank} \bullet \mathrm{charge2}?\langle x_{c2}, x_{cc}, x_{amount}\rangle.s_2 \,) \\
\mid \; (\, \mathrm{bank} \bullet \mathrm{charge1}?\langle x_{c1}, 1234, 100€, x_{info}\rangle.s_1 \;\mid\; s_2 \,) \cdot \{\cdots \mapsto \cdots\} \\
\mid \; (\, \mathrm{bank} \bullet \mathrm{charge1}!\langle c_1, 1234, 100€, \mathrm{info}\rangle \;\mid\; s'_1 \,) \;\mid\; (\, s'_2 \,)
\end{array}
$$

μCOWS: *joint account* service example



$$
\begin{array}{l}
* \, [x_{c1}, x_{c2}, x_{cc}, x_{amount}, x_{info}] \, (\, \mathrm{bank} \bullet \mathrm{charge1}?\langle x_{c1}, x_{cc}, x_{amount}, x_{info} \rangle . s_1 \\
\qquad\qquad\qquad\qquad\qquad \mid \ \mathrm{bank} \bullet \mathrm{charge2}?\langle x_{c2}, x_{cc}, x_{amount} \rangle . s_2 \,) \\
\mid \ (\, \mathrm{bank} \bullet \mathrm{charge1}?\langle x_{c1}, 1234, 100€, x_{info} \rangle . s_1 \ \mid \ s_2 \,) \cdot \{ \cdots \mapsto \cdots \} \\
\mid \ (\, \mathrm{bank} \bullet \mathrm{charge1}!\langle c_1, 1234, 100€, \mathrm{info} \rangle \ \mid \ s'_1 \,) \ \mid \ (\, s'_2 \,)
\end{array}
$$

μCOWS: *joint account* service example



$$
\begin{aligned}
* \, [x_{c1}, x_{c2}, x_{cc}, x_{amount}, x_{info}] \, (& \, \mathsf{bank} \bullet \mathsf{charge1}?\langle x_{c1}, x_{cc}, x_{amount}, x_{info} \rangle . s_1 \\
& \mid \mathsf{bank} \bullet \mathsf{charge2}?\langle x_{c2}, x_{cc}, x_{amount} \rangle . s_2 \,) \\
\mid \; (\, s_1 \mid s_2 \,) \cdot \{ \cdots \mapsto \cdots \} & \\
\mid \; (\, s'_1 \,) \mid (\, s'_2 \,) &
\end{aligned}
$$

Parallel with priority as a coordination mechanism

Default behaviour

Consider a service providing mathematical functionalities
e.g. sum of two integers between 0 and 5

$$
\begin{aligned}
*\,[x,y,z]\,(\,& \mathit{math} \bullet \mathit{sum}?\langle x,y,z\rangle.\, x \bullet \mathit{resp}!\langle \mathit{error}\rangle \\
& + \ \mathit{math} \bullet \mathit{sum}?\langle x,0,0\rangle.\, x \bullet \mathit{resp}!\langle 0\rangle \\
& + \ \mathit{math} \bullet \mathit{sum}?\langle x,0,1\rangle.\, x \bullet \mathit{resp}!\langle 1\rangle \\
& + \ \ldots + \ \mathit{math} \bullet \mathit{sum}?\langle x,5,5\rangle.\, x \bullet \mathit{resp}!\langle 10\rangle\ )
\end{aligned}
$$

In case the two values are not admissible, i.e. they are not integers between 0 and 5, the service replies with the string *error*

Parallel with priority as a coordination mechanism

‘Only the first time’ behaviour

Consider a service that has a certain behaviour at the first correct invocation and a different behaviour at any incorrect or further invocation
(useful, e.g., for compensation handling à la WS-BPEL)

$$\begin{array}{l} p \bullet comp?\langle scopeName \rangle . \langle \text{compensation of } scopeName \rangle \\ \mid \; *\, [x]\, p \bullet comp?\langle x \rangle . \langle \text{do nothing} \rangle \end{array}$$

Parallel with priority as a coordination mechanism

'Blind date' session joining

Consider a service capable of arranging matches of 4-players online games

$$
\begin{aligned}
\mathit{masterServ} \triangleq\ * \,[x_{game}, x_{player1}, x_{player2}, x_{player3}, x_{player4}]\ & \\
& \mathit{master} \bullet \mathit{join}?\langle x_{game}, x_{player1}\rangle. \\
& \mathit{master} \bullet \mathit{join}?\langle x_{game}, x_{player2}\rangle. \\
& \mathit{master} \bullet \mathit{join}?\langle x_{game}, x_{player3}\rangle. \\
& \mathit{master} \bullet \mathit{join}?\langle x_{game}, x_{player4}\rangle. \\
& \quad [\mathit{matchId}]\,(\, x_{player1} \bullet \mathit{start}!\langle \mathit{matchId}\rangle \\
& \qquad\qquad\qquad \mid x_{player2} \bullet \mathit{start}!\langle \mathit{matchId}\rangle \\
& \qquad\qquad\qquad \mid x_{player3} \bullet \mathit{start}!\langle \mathit{matchId}\rangle \\
& \qquad\qquad\qquad \mid x_{player4} \bullet \mathit{start}!\langle \mathit{matchId}\rangle\,)
\end{aligned}
$$

$$\mathit{Player}_i \triangleq \mathit{master} \bullet \mathit{join}!\langle \mathit{poker}, p_i\rangle \mid [x_{id}]\, p_i \bullet \mathit{start}?\langle x_{id}\rangle.\ \langle \text{rest of } \mathit{Player}_i\rangle$$

$$\mathit{Player}_j \triangleq \mathit{master} \bullet \mathit{join}!\langle \mathit{bridge}, p_j\rangle \mid [x_{id}]\, p_j \bullet \mathit{start}?\langle x_{id}\rangle.\ \langle \text{rest of } \mathit{Player}_j\rangle$$

It could be hard to render this behaviour with other process calculi

Parallel with priority as a coordination mechanism

'Blind date' session joining

Consider a service capable of arranging matches of 4-players online games

$$
\begin{aligned}
\textit{masterServ} \triangleq\ * [x_{game}, x_{player1}, x_{player2}, x_{player3}, x_{player4}]\\
& \textit{master} \bullet \textit{join}?\langle x_{game}, x_{player1}\rangle.\\
& \textit{master} \bullet \textit{join}?\langle x_{game}, x_{player2}\rangle.\\
& \textit{master} \bullet \textit{join}?\langle x_{game}, x_{player3}\rangle.\\
& \textit{master} \bullet \textit{join}?\langle x_{game}, x_{player4}\rangle.\\
& \quad [\textit{matchId}]\,(\, x_{player1} \bullet \textit{start}!\langle \textit{matchId}\rangle\\
& \quad\quad \mid x_{player2} \bullet \textit{start}!\langle \textit{matchId}\rangle\\
& \quad\quad \mid x_{player3} \bullet \textit{start}!\langle \textit{matchId}\rangle\\
& \quad\quad \mid x_{player4} \bullet \textit{start}!\langle \textit{matchId}\rangle\,)
\end{aligned}
$$

$$\textit{Player}_i \triangleq \textit{master} \bullet \textit{join}!\langle \textit{poker}, p_i\rangle \mid [x_{id}]\, p_i \bullet \textit{start}?\langle x_{id}\rangle.\,\langle \text{rest of } \textit{Player}_i\rangle$$

$$\textit{Player}_j \triangleq \textit{master} \bullet \textit{join}!\langle \textit{bridge}, p_j\rangle \mid [x_{id}]\, p_j \bullet \textit{start}?\langle x_{id}\rangle.\,\langle \text{rest of } \textit{Player}_j\rangle$$

It could be hard to render this behaviour with other process calculi

From μCOWS to COWS

μCOWS

From μCOWS to COWS

μCOWS

+

Termination activities

From μCOWS to COWS

μCOWS

+

Termination activities

=

COWS

COWS: why termination activities?

1. To handle *faults* and enable *compensation*

2. Termination activities can be used as *orchestration mechanisms*
   - E.g. to model the asymmetric parallel composition of Orc (i.e. the *pruning* construct, that prunes threads selectively)

Syntax of COWS

$s ::=$		(services)
	$\mathbf{kill}(k)$	(kill)
$\mid$	$u \bullet u' ! \bar{\epsilon}$	(invoke)
$\mid$	$\sum_{i=0}^{r} g_i . s_i$	(receive-guarded choice)
$\mid$	$s \mid s$	(parallel composition)
$\mid$	$\{\mid s \mid\}$	(protection)
$\mid$	$[e]\, s$	(delimitation)
$\mid$	$* s$	(replication)
$g ::=$		(guards)
	$p \bullet o ? \bar{w}$	(receive)

(notations)
k: (killer) labels
ϵ: *expressions*
x: *variables*
v: *values*
n, p, o: *names*
u: *variables* | *names*
w: *variables* | *values*
e: *labels* | *variables* | *names*

- Killer labels cannot occur within expressions
  $\Rightarrow$ they are not (communicable) values
- Only one binding construct: $[e]\, s$ binds e in the scope s
  - free/bound *elements* (i.e. names/variables/labels) defined accordingly

COWS operational semantics

Additional structural congruence laws

- $\{\!|\mathbf{0}|\!\} \;\equiv\; \mathbf{0} \qquad \{\!|\, \{\!|s|\!\}\, |\!\} \;\equiv\; \{\!|s|\!\} \qquad \{\!|[e]\,s|\!\} \;\equiv\; [e]\,\{\!|s|\!\}$
- $s_1 \mid [e]\,s_2 \;\equiv\; [e]\,(s_1 \mid s_2) \quad \text{if } e \notin \mathrm{fe}(s_1) \cup \mathrm{fk}(s_2)$
  - $\mathrm{fe}(s)$ denotes the set of elements occurring free in s
  - $\mathrm{fk}(s)$ denotes the set of free killer labels in s
  - thus, differently from names/variables, the scope of killer labels cannot be extended

Labelled transition relation $\xrightarrow{\alpha}$

Label α is now generated by the following grammar:

$$\alpha \;::=\; \mathrm{n} \lhd \bar{v} \;\mid\; \mathrm{n} \rhd \bar{w} \;\mid\; \mathrm{n}\,\sigma\,\ell\,\bar{v} \;\mid\; k \;\mid\; \dagger$$

COWS: Kill activity

- Activity **kill**(k) forces termination of all unprotected parallel activities inside an enclosing $[k]$, that stops the killing effect

$$\mathbf{kill}(k) \xrightarrow{k} \mathbf{0} \qquad \frac{s_1 \xrightarrow{k} s_1'}{s_1 \mid s_2 \xrightarrow{k} s_1' \mid \mathrm{halt}(s_2)} \qquad \frac{s \xrightarrow{k} s'}{[k]\, s \xrightarrow{\dagger} [k]\, s'}$$

COWS: Kill activity

- Activity $\mathbf{kill}(k)$ forces termination of all unprotected parallel activities inside an enclosing $[k]$, that stops the killing effect

$$\mathbf{kill}(k) \xrightarrow{k} \mathbf{0} \qquad \frac{s_1 \xrightarrow{k} s_1'}{s_1 \mid s_2 \xrightarrow{k} s_1' \mid \mathrm{halt}(s_2)} \qquad \frac{s \xrightarrow{k} s'}{[k]\, s \xrightarrow{\dagger} [k]\, s'}$$

Function $\mathrm{halt}(s)$

returns the service obtained by only retaining the protected activities inside s

$$\mathrm{halt}(\mathbf{kill}(k)) \;=\; \mathrm{halt}(\mathtt{u}!\bar{\epsilon}) \;=\; \mathrm{halt}(\textstyle\sum_{i=0}^{r} \mathtt{n}_i?\bar{w}_i.s_i) \;=\; \mathbf{0}$$

$$\mathrm{halt}(s_1 \mid s_2) = \mathrm{halt}(s_1) \mid \mathrm{halt}(s_2) \qquad \mathrm{halt}(\{\!|s|\!\}) = \{\!|s|\!\}$$

$$\mathrm{halt}([e]\, s) = [e]\, \mathrm{halt}(s) \qquad \mathrm{halt}(*\, s) = *\, \mathrm{halt}(s)$$

COWS: Kill activity

- Activity **kill**(k) forces termination of all unprotected parallel activities inside an enclosing $[k]$, that stops the killing effect

$$\mathbf{kill}(k) \xrightarrow{k} \mathbf{0} \qquad \frac{s_1 \xrightarrow{k} s_1'}{s_1 \mid s_2 \xrightarrow{k} s_1' \mid \mathrm{halt}(s_2)} \qquad \frac{s \xrightarrow{k} s'}{[k]\, s \xrightarrow{\dagger} [k]\, s'}$$

- Kill activities are executed *eagerly*

$$\frac{s \xrightarrow{k} s' \quad k \neq e}{[e]\, s \xrightarrow{k} [e]\, s'} \qquad \frac{s \xrightarrow{\dagger} s'}{[e]\, s \xrightarrow{\dagger} [e]\, s'}$$

$$\frac{s \xrightarrow{\alpha} s' \quad e \notin \mathrm{e}(\alpha) \quad \alpha \neq k, \dagger \quad \mathrm{noKill}(s, e)}{[e]\, s \xrightarrow{\alpha} [e]\, s'}$$

COWS: Kill activity

- Activity **kill**(k) forces termination of all unprotected parallel activities inside an enclosing $[k]$, that stops the killing effect
- Kill activities are executed *eagerly*

$$\frac{s \xrightarrow{k} s' \quad k \neq e}{[e]\, s \xrightarrow{k} [e]\, s'} \qquad \frac{s \xrightarrow{\dagger} s'}{[e]\, s \xrightarrow{\dagger} [e]\, s'}$$

$$\frac{s \xrightarrow{\alpha} s' \quad e \notin \mathrm{e}(\alpha) \quad \alpha \neq k, \dagger \quad \mathrm{noKill}(s, e)}{[e]\, s \xrightarrow{\alpha} [e]\, s'}$$

Predicate $\mathrm{noKill}(s, e)$ (part 1/2)

checks the ability of s of immediately performing a kill activity

$$\mathrm{noKill}(s, e) = \textbf{true} \quad \text{if } \mathrm{fk}(e) = \emptyset \qquad \mathrm{noKill}(\textbf{kill}(k'), k) = \textbf{true} \quad \text{if } k \neq k'$$

$$\mathrm{noKill}(\textbf{kill}(k), k) = \textbf{false} \qquad \mathrm{noKill}(\mathrm{u}!\bar{\epsilon}, k) = \mathrm{noKill}(\textstyle\sum_{i=0}^{r} \mathrm{n}_i?\bar{w}_i.s_i, k) = \textbf{true}$$

COWS: Kill activity

- Activity **kill**(k) forces termination of all unprotected parallel activities inside an enclosing $[k]$, that stops the killing effect
- Kill activities are executed *eagerly*

$$\frac{s \xrightarrow{k} s' \quad k \neq e}{[e]\, s \xrightarrow{k} [e]\, s'} \qquad \frac{s \xrightarrow{\dagger} s'}{[e]\, s \xrightarrow{\dagger} [e]\, s'}$$

$$\frac{s \xrightarrow{\alpha} s' \quad e \notin \mathrm{e}(\alpha) \quad \alpha \neq k, \dagger \quad \mathrm{noKill}(s, e)}{[e]\, s \xrightarrow{\alpha} [e]\, s'}$$

Predicate $\mathrm{noKill}(s, e)$ (part 2/2)

checks the ability of s of immediately performing a kill activity

$\mathrm{noKill}(s \mid s', k) = \mathrm{noKill}(s, k) \wedge \mathrm{noKill}(s', k) \quad \mathrm{noKill}([e]\, s, k) = \mathrm{noKill}(s, k)$ if $e \neq k$

$\mathrm{noKill}([k]\, s, k) = \textbf{true} \qquad \mathrm{noKill}(\{|s|\}, k) = \mathrm{noKill}(*\, s, k) = \mathrm{noKill}(s, k)$

COWS: Kill activity

- Activity **kill**(k) forces termination of all unprotected parallel activities inside an enclosing $[k]$, that stops the killing effect
- Kill activities are executed *eagerly*
- $\{\!|\cdot|\!\}$ protects activities from the effect of a forced termination

$$\frac{s \xrightarrow{\alpha} s'}{\{\!|s|\!\} \xrightarrow{\alpha} \{\!|s'|\!\}}$$

COWS operational semantics: labelled transition rules

$$\frac{[\![\bar{\epsilon}]\!] = \bar{v}}{\mathrm{n}!\bar{\epsilon} \xrightarrow{\mathrm{n} \lhd \bar{v}} \mathbf{0}} \qquad \frac{1 \leq j \leq r}{\sum_{i=1}^{r} \mathrm{n}_i?\bar{w}_i.s_i \xrightarrow{\mathrm{n}_j \rhd \bar{w}_j} s_j} \qquad \frac{s \equiv \xrightarrow{\alpha} \equiv s'}{s \xrightarrow{\alpha} s'}$$

$$\frac{s_1 \xrightarrow{\mathrm{n} \rhd \bar{w}} s_1' \quad s_2 \xrightarrow{\mathrm{n} \lhd \bar{v}} s_2' \quad \mathcal{M}(\bar{w}, \bar{v}) = \sigma \quad \mathrm{noConf}(s_1 \mid s_2, \mathrm{n}, \bar{v}, |\sigma|)}{s_1 \mid s_2 \xrightarrow{\mathrm{n}\, \sigma\, |\sigma|\, \bar{v}} s_1' \mid s_2'}$$

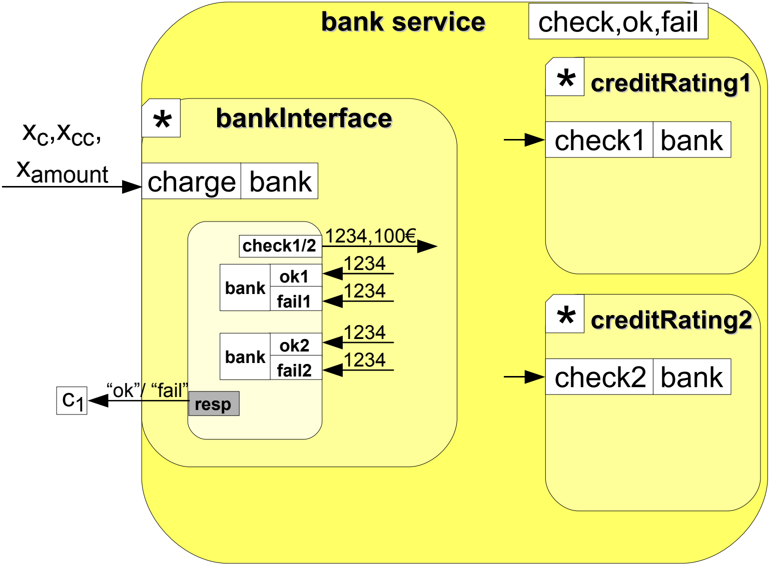
$$\frac{s \xrightarrow{\mathrm{n}\, \sigma \uplus \{x \mapsto v\}\, \ell\, \bar{v}} s'}{[x]\, s \xrightarrow{\mathrm{n}\, \sigma\, \ell\, \bar{v}} s' \cdot \{x \mapsto v\}} \qquad \frac{s_1 \xrightarrow{\mathrm{n}\, \sigma\, \ell\, \bar{v}} s_1' \quad \mathrm{noConf}(s_2, \mathrm{n}, \bar{v}, \ell)}{s_1 \mid s_2 \xrightarrow{\mathrm{n}\, \sigma\, \ell\, \bar{v}} s_1' \mid s_2}$$

$$\mathbf{kill}(k) \xrightarrow{k} \mathbf{0} \qquad \frac{s \xrightarrow{\alpha} s'}{\{\!|s|\!\} \xrightarrow{\alpha} \{\!|s'|\!\}} \qquad \frac{s_1 \xrightarrow{\alpha} s_1' \quad \alpha \neq k, \mathrm{n}\, \sigma\, \ell\, \bar{v}}{s_1 \mid s_2 \xrightarrow{\alpha} s_1' \mid s_2}$$

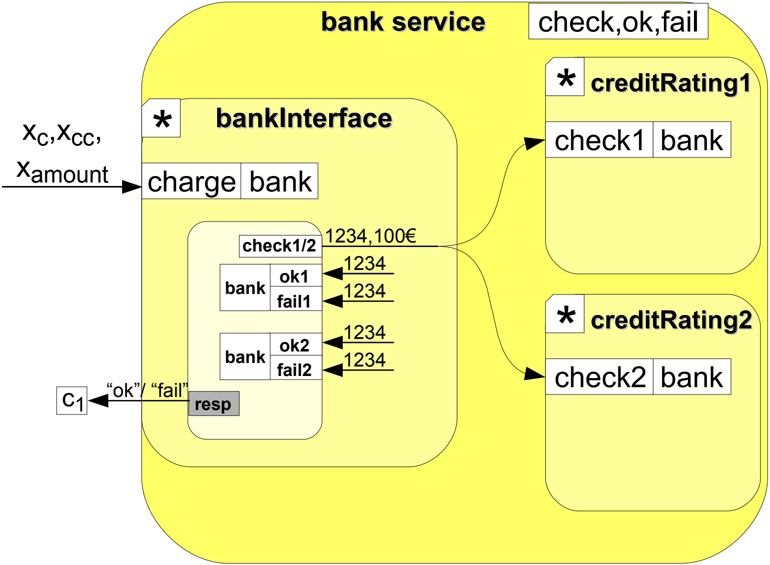
$$\frac{s \xrightarrow{k} s'}{[k]\, s \xrightarrow{\dagger} [k]\, s'} \qquad \frac{s \xrightarrow{k} s' \quad k \neq e}{[e]\, s \xrightarrow{k} [e]\, s'} \qquad \frac{s_1 \xrightarrow{k} s_1'}{s_1 \mid s_2 \xrightarrow{k} s_1' \mid \mathrm{halt}(s_2)}$$

$$\frac{s \xrightarrow{\dagger} s'}{[e]\, s \xrightarrow{\dagger} [e]\, s'} \qquad \frac{s \xrightarrow{\alpha} s' \quad e \notin \mathrm{e}(\alpha) \quad \alpha \neq k, \dagger \quad \mathrm{noKill}(s, e)}{[e]\, s \xrightarrow{\alpha} [e]\, s'}$$

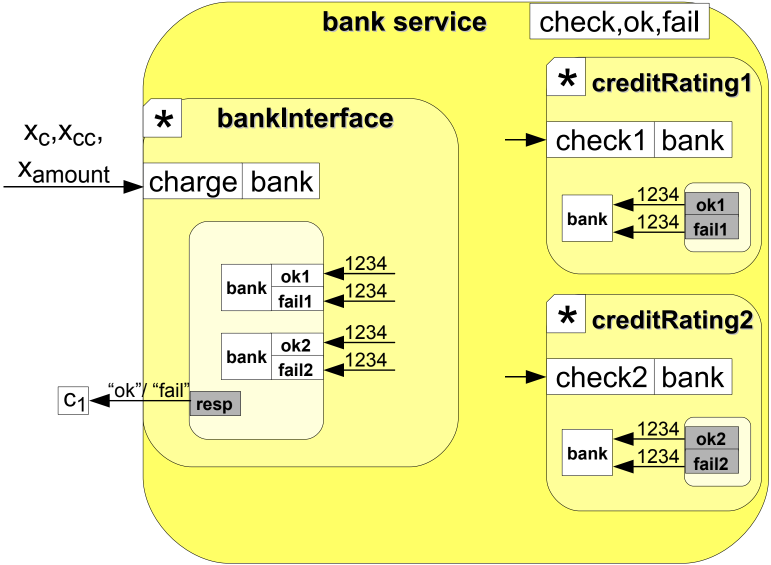
COWS: *multi rating* bank service example



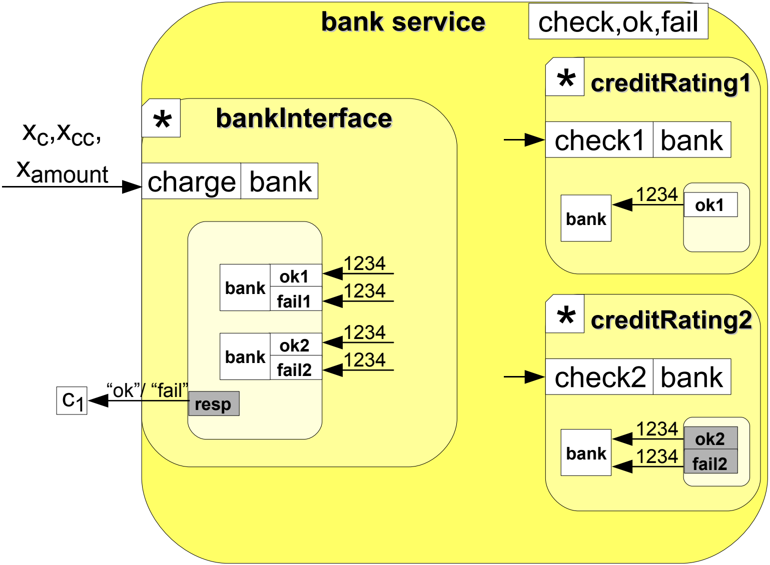
COWS: *multi rating* bank service example



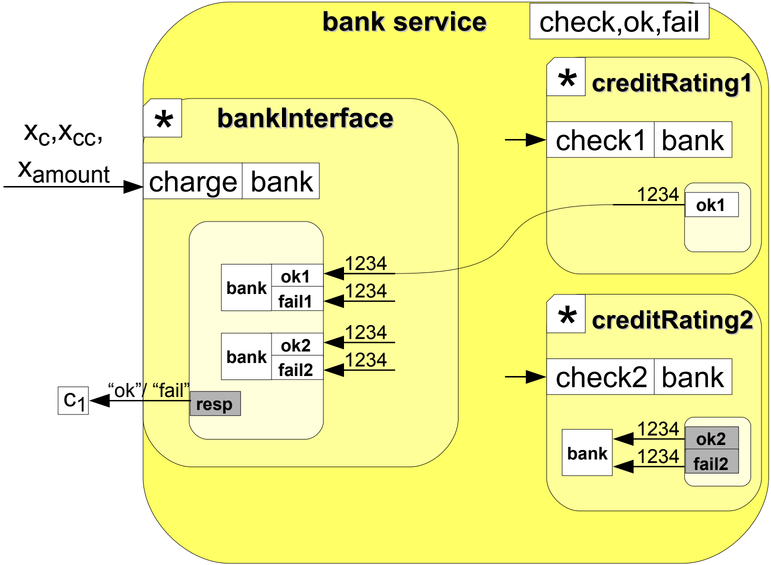
COWS: *multi rating* bank service example



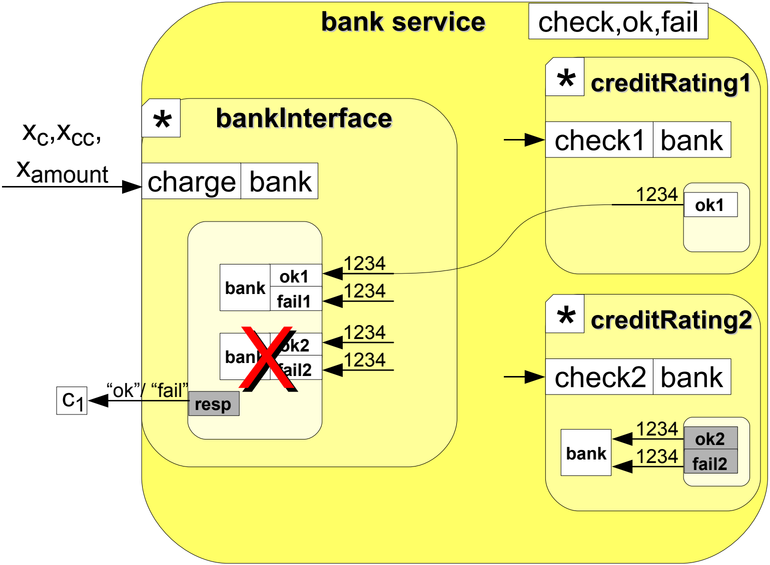
COWS: *multi rating* bank service example



COWS: *multi rating* bank service example



COWS: *multi rating* bank service example



COWS: *multi rating* bank service example

$$[\mathrm{check1}, \mathrm{check2}, \mathrm{ok1}, \mathrm{ok2}, \mathrm{fail1}, \mathrm{fail2}]$$
$$(\, * \,\mathrm{bankInterface} \mid * \,\mathrm{creditRating1} \mid * \,\mathrm{creditRating2}\,)$$

$$
\begin{array}{l}
\mathrm{bankInterface} \;\triangleq \\
\quad [\mathrm{x_c}, \mathrm{x_{cc}}, \mathrm{x_{amount}}] \\
\quad \mathrm{bank} \bullet \mathrm{charge}?\langle \mathrm{x_c}, \mathrm{x_{cc}}, \mathrm{x_{amount}} \rangle. \\
\quad (\, \mathrm{bank} \bullet \mathrm{check1}!\langle \mathrm{x_{cc}}, \mathrm{x_{amount}} \rangle \mid \mathrm{bank} \bullet \mathrm{check2}!\langle \mathrm{x_{cc}}, \mathrm{x_{amount}} \rangle \\
\quad\;\; \mid [k]\,(\, \mathrm{bank} \bullet \mathrm{ok1}?\langle \mathrm{x_{cc}} \rangle.\,(\, \mathbf{kill}(k) \mid \{\!|\, \mathrm{x_c} \bullet \mathrm{resp}!\langle \text{“ok”} \rangle \,|\!\}\,) \\
\qquad\qquad\quad + \mathrm{bank} \bullet \mathrm{fail1}?\langle \mathrm{x_{cc}} \rangle.\, s_1 \\
\qquad\qquad \mid \mathrm{bank} \bullet \mathrm{ok2}?\langle \mathrm{x_{cc}} \rangle.\,(\, \mathbf{kill}(k) \mid \{\!|\, \mathrm{x_c} \bullet \mathrm{resp}!\langle \text{“ok”} \rangle \,|\!\}\,) \\
\qquad\qquad\quad + \mathrm{bank} \bullet \mathrm{fail2}?\langle \mathrm{x_{cc}} \rangle.\, s_2 \,)\,)
\end{array}
$$

COWS: peculiar examples

Protected kill activity

- Execution of a kill activity within a protection block

$$[k]\,(\{\!|s_1 \mid \{\!|s_2|\!\} \mid \mathbf{kill}(k)|\!\} \mid s_3) \mid s_4 \xrightarrow{\dagger} [k]\,\{\!|s_2|\!\} \mid s_4$$

For simplicity, assume that $\mathrm{halt}(s_1) = \mathrm{halt}(s_3) = \mathbf{0}$

- **kill**(k) terminates all parallel services inside delimitation $[k]$ (i.e. s_1 and s_3), except those that are protected at the same nesting level of the kill activity (i.e. s_2)

COWS: peculiar examples

Protected kill activity

- Execution of a kill activity within a protection block

$$[k]\,(\{\!|s_1 \;|\; \{\!|s_2|\!\} \;|\; \mathbf{kill}(k)|\!\} \;|\; s_3) \;|\; s_4 \xrightarrow{\dagger} [k]\,\{\!|s_2|\!\} \;|\; s_4$$

For simplicity, assume that $\mathrm{halt}(s_1) = \mathrm{halt}(s_3) = \mathbf{0}$

- $\mathbf{kill}(k)$ terminates all parallel services inside delimitation $[k]$ (i.e. s_1 and s_3), except those that are protected at the same nesting level of the kill activity (i.e. s_2)

COWS: peculiar examples

Protected kill activity

- Execution of a kill activity within a protection block

$$[k]\,(\{\!|s_1 \;\mid\; \{\!|s_2|\!\} \;\mid\; \mathbf{kill}(k)|\!\} \;\mid\; s_3) \;\mid\; s_4 \xrightarrow{\dagger} [k]\,\{\!|s_2|\!\} \;\mid\; s_4$$

  For simplicity, assume that $\mathrm{halt}(s_1) = \mathrm{halt}(s_3) = \mathbf{0}$

- $\mathbf{kill}(k)$ terminates all parallel services inside delimitation $[k]$ (i.e. s_1 and s_3), except those that are protected at the same nesting level of the kill activity (i.e. s_2)

COWS: peculiar examples

Interplay between communication and kill activity

$$p \bullet o!\langle n \rangle \mid [k]\,([x]\,p \bullet o?\langle x \rangle.s \mid \mathbf{kill}(k)) \xrightarrow{\dagger} p \bullet o!\langle n \rangle \mid [k]\,[x]\,\mathbf{0}$$

- Kill activities can break communication
- This is the only possible evolution (kills are executed *eagerly*)
- Communication can be guaranteed by protecting the receive

$$p \bullet o!\langle n \rangle \mid [k]\,([x]\,\{\!|p \bullet o?\langle x \rangle.s|\!\} \mid \mathbf{kill}(k)) \xrightarrow{\dagger}$$

$$p \bullet o!\langle n \rangle \mid [k]\,([x]\,\{\!|p \bullet o?\langle x \rangle.s|\!\}) \xrightarrow{p \bullet o\,\emptyset\,1\,\langle n \rangle} [k]\,\{\!|s \cdot \{x \mapsto n\}|\!\}$$

COWS: peculiar examples

Interplay between communication and kill activity

$$p \bullet o!\langle n\rangle \mid [k]\,([x]\,p \bullet o?\langle x\rangle.s \mid \mathbf{kill}(k)) \xrightarrow{\dagger} p \bullet o!\langle n\rangle \mid [k]\,[x]\,\mathbf{0}$$

- Kill activities can break communication
- This is the only possible evolution (kills are executed *eagerly*)
- Communication can be guaranteed by protecting the receive

$$p \bullet o!\langle n\rangle \mid [k]\,([x]\,\{\!|p \bullet o?\langle x\rangle.s|\!\} \mid \mathbf{kill}(k)) \xrightarrow{\dagger}$$

$$p \bullet o!\langle n\rangle \mid [k]\,([x]\,\{\!|p \bullet o?\langle x\rangle.s|\!\}) \xrightarrow{p \bullet o\,\emptyset\,1\,\langle n\rangle} [k]\,\{\!|s \cdot \{x \mapsto n\}|\!\}$$

COWS expressiveness

Considerations on COWS expressiveness

- Encoding other calculi
  - π-calculus, Localized π-calculus (Lπ), ...
  - SCC (Session Centered Calculus)
  - Orc
  - WS-CALCULUS
  - B*lite* (a lightweight version of WS-BPEL)
- COWS (like other calculi equipped with priority) is not encodable into mainstream calculi (e.g. CCS and π-calculus) [EXPRESS'10]
- Modelling imperative and orchestration constructs
  - Assignment, conditional choice, sequential composition,...
  - WS-BPEL flow graphs, fault and compensation handlers
  - QoS requirement specifications and SLA negotiations [WWV'07]
  - Timed orchestration constructs [ICTAC'07]

Considerations on COWS expressiveness

- Encoding other calculi
  - π-calculus, Localized π-calculus (Lπ), ...
  - SCC (Session Centered Calculus)
  - Orc
  - WS-CALCULUS
  - B*lite* (a lightweight version of WS-BPEL)

- COWS (like other calculi equipped with priority) is not encodable into mainstream calculi (e.g. CCS and π-calculus) [EXPRESS'10]

- Modelling imperative and orchestration constructs
  - Assignment, conditional choice, sequential composition,...
  - WS-BPEL flow graphs, fault and compensation handlers
  - QoS requirement specifications and SLA negotiations [WWV'07]
  - Timed orchestration constructs [ICTAC'07]

Considerations on COWS expressiveness

- Encoding other calculi
  - π-calculus, Localized π-calculus (Lπ), ...
  - SCC (Session Centered Calculus)
  - Orc
  - WS-CALCULUS
  - B*lite* (a lightweight version of WS-BPEL)

- COWS (like other calculi equipped with priority) is not encodable into mainstream calculi (e.g. CCS and π-calculus) [EXPRESS'10]

- Modelling imperative and orchestration constructs
  - Assignment, conditional choice, sequential composition,...
  - WS-BPEL flow graphs, fault and compensation handlers
  - QoS requirement specifications and SLA negotiations [WWV'07]
  - Timed orchestration constructs [ICTAC'07]

References

References 1/4

A WSDL-based type system for WS-BPEL
A. Lapadula, R. Pugliese, F. Tiezzi. Proc. of COORDINATION’06, LNCS 4038, 2006.

A calculus for orchestration of web services
A. Lapadula, R. Pugliese, F. Tiezzi. Proc. of ESOP’07, LNCS 4421, 2007.

go back

Regulating data exchange in service oriented applications
A. Lapadula, R. Pugliese, F. Tiezzi. Proc. of FSEN’07, LNCS 4767, 2007.

go back

COWS: A timed service-oriented calculus
A. Lapadula, R. Pugliese, F. Tiezzi. Proc. of ICTAC’07, LNCS 4711, 2007.

go back

Stochastic COWS
D. Prandi, P. Quaglia. Proc. of ICSOC’07, LNCS 4749, 2007.

References 2/4

- A model checking approach for verifying COWS specifications
  A. Fantechi, S. Gnesi, A. Lapadula, F. Mazzanti, R. Pugliese, F. Tiezzi.
  Proc. of FASE'08, LNCS 4961, 2008. go back

- Service discovery and negotiation with COWS
  A. Lapadula, R. Pugliese, F. Tiezzi. Proc. of WWV'07, ENTCS 200(3), 2008. go back

- Specifying and Analysing SOC Applications with COWS
  A. Lapadula, R. Pugliese, F. Tiezzi. In Concurrency, Graphs and Models, LNCS 5065, 2008.

- SENSORIA Patterns: Augmenting Service Engineering with Formal Analysis, Transformation and Dynamicity
  M. Wirsing, et al. Proc. of ISOLA'08, Communications in Computer and Information Science 17, 2008.

- A formal account of WS-BPEL
  A. Lapadula, R. Pugliese, F. Tiezzi. Proc. of COORDINATION'08, LNCS 5052, 2008.

References 3/4

- Formal analysis of BPMN via a translation into COWS
  D. Prandi, P. Quaglia, N. Zannone. Proc. of COORDINATION'08, LNCS 5052, 2008.

- Relational Analysis of Correlation
  J. Bauer, F. Nielson, H.R. Nielson, H. Pilegaard. Proc. of SAS'08, LNCS 5079, 2008.

- A Symbolic Semantics for a Calculus for Service-Oriented Computing
  R. Pugliese, F. Tiezzi, N. Yoshida. Proc. of PLACES'08, ENTCS 241, 2009.

- Specification and analysis of SOC systems using COWS: A finance case study
  F. Banti, A. Lapadula, R. Pugliese, F. Tiezzi. Proc. of WWV'08, ENTCS 235(C), 2009.

- From Architectural to Behavioural Specification of Services
  L. Bocchi, J.L. Fiadeiro, A. Lapadula, R. Pugliese, F. Tiezzi. Proc. of FESCA'09, ENTCS 253/1, 2009.

References 4/4

- On observing dynamic prioritised actions in SOC
  R. Pugliese, F. Tiezzi, N. Yoshida. Proc. of ICALP'09, LNCS 5556, 2009.
  go back

- On secure implementation of an IHE XUA-based protocol for authenticating healthcare professionals
  M. Masi, R. Pugliese, F. Tiezzi. Proc. of ICISS'09, LNCS 5905, 2009.

- Rigorous Software Engineering for Service-Oriented Systems - Results of the SENSORIA Project on Software Engineering for Service-Oriented Computing
  M. Wirsing and M. Hölzl Editors. LNCS, 2010. To appear.

- An Accessible Verification Environment for UML Models of Services
  F. Banti, R. Pugliese, F. Tiezzi. Journal of Symbolic Computation, 2010. To appear.

- A criterion for separating process calculi
  F. Banti, R. Pugliese, F. Tiezzi. Proc. of EXPRESS'10, 2010. go back