The Marriage of Compass and Mils

Soul mates find one another

Once upon a time …

a wise and learned Englishman had a daughter. Born in 1981, a separation kernel she was. By her early 20's she had developed maturity and was followed by many suitors. At her coming out, she took the name "Mils", and her father was very proud of the attention she received.

Mils had shared her dreams with family and friends. She pondered great problems, thinking carefully about how she could solve them, but she couldn't implement these ideas all by herself.

She wasn't interested in the casual and shallow suitors. Mils longed for a real partner with depth, with whom to build a life. (Secretly, she worried that she would become an Old Maid.)

Meanwhile, in another land …

a union of great European families had produced an agile and strong young builder named Compass. In addition to his athleticism, he had an elegant way of expressing himself in a language that Mils had dreamed of one day learning.

Already, Compass' accomplishments were remarkable, helping to build things to go into space, and he and his family were rightfully very proud. But Compass longed for a life partner who would love him for who he was, not just what he could do.

And so Compass continued to hone his skills, build things, and speak far and wide of his fascinating accomplishments.

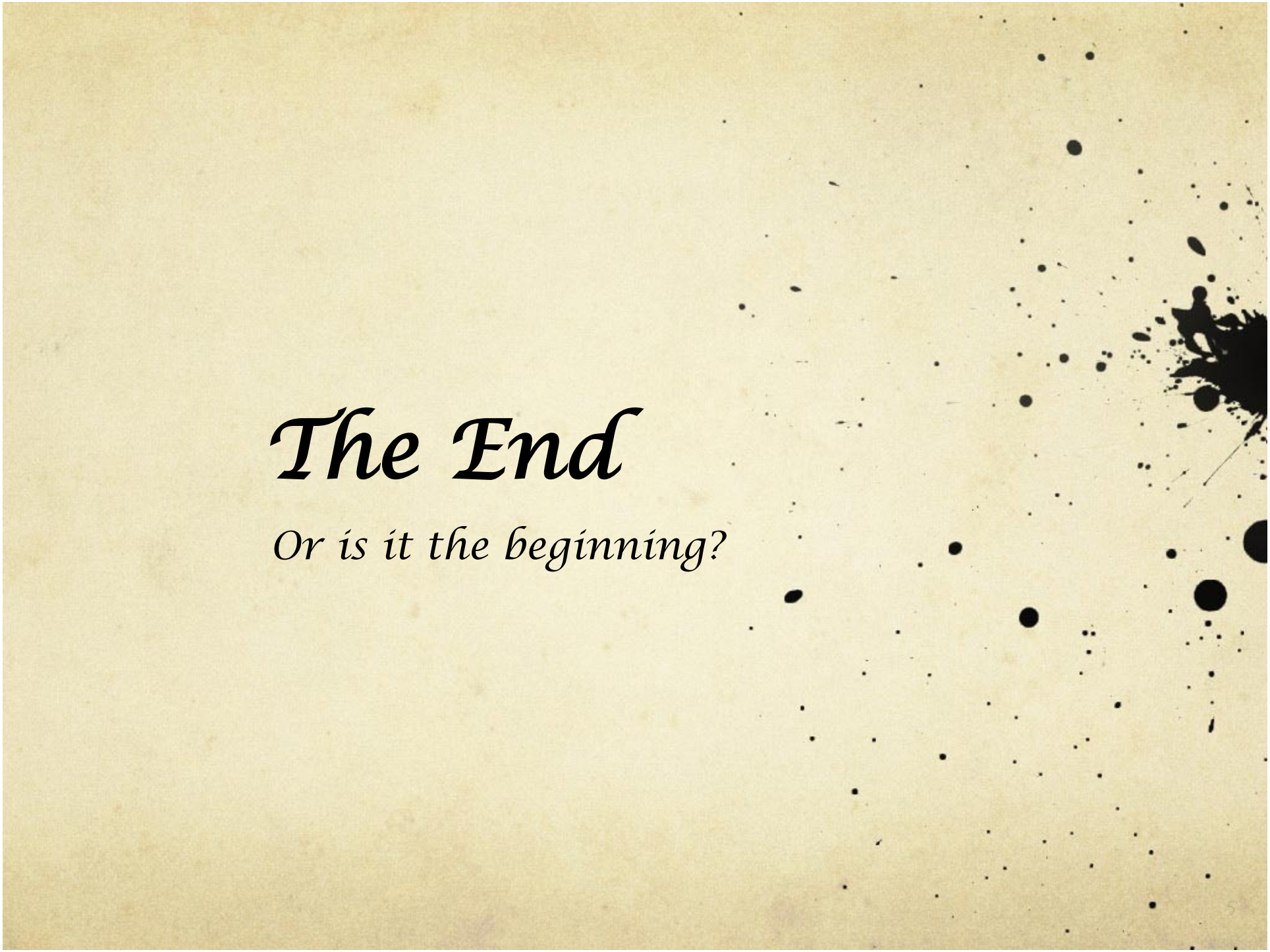
Then, one enchanted evening …

in 2011, in a beautiful city by a river at the foot of great mountains in northern Italy, Compass and Mils were introduced at the FMICS Ball. Compass exhibited his gift for expression, as well as his strength and agility on the dance floor. Mils marveled at Compass, and with racing heart began to tell him of all her grand ideas and plans.

The two quickly developed a bond, and soon entered into a contract of engagement with the Dowry of Mils (D-MILS).

Now, celebrating their union, Compass and Mils look forward to facing together the greatest challenges of life in a dynamic world.

And they lived happily ever after.

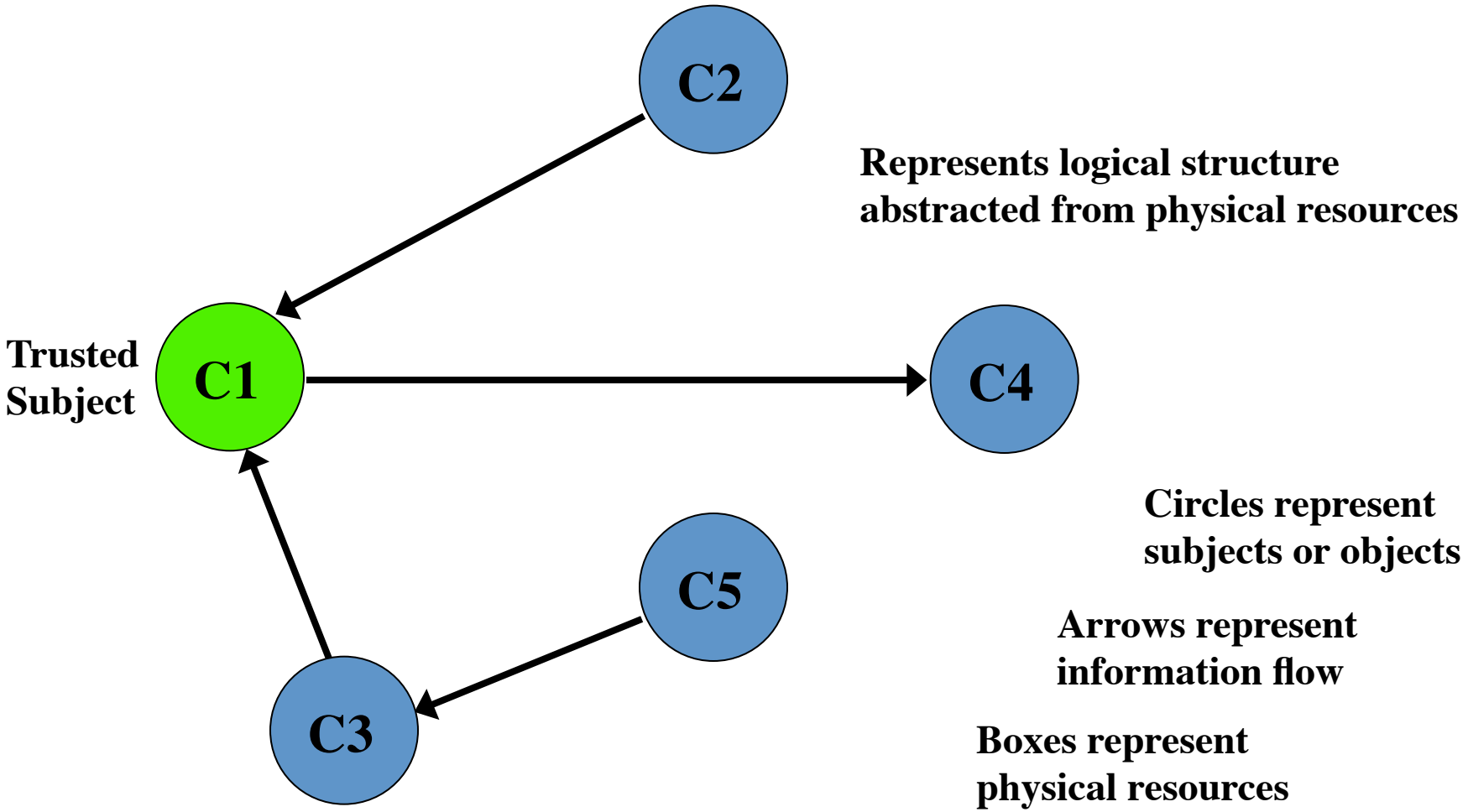

The End
Or is it the beginning?

The Marriage of COMPASS and MILS

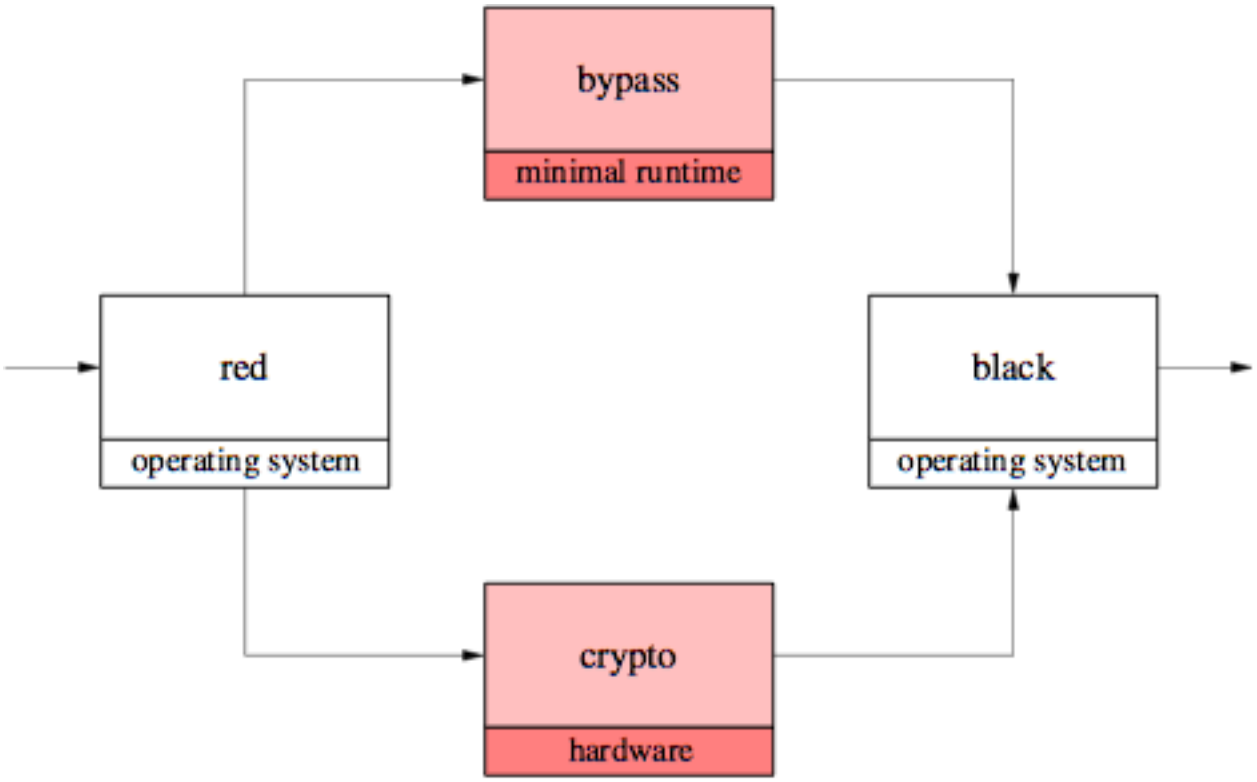
Fairy tales aside, …

The following few slides from MILS presentations, exhibit MILS' aspirations, prior to meeting COMPASS:

MILS Policy Architecture -- Diagram Showing System Decomposition



Secure Network Front End* architecture view



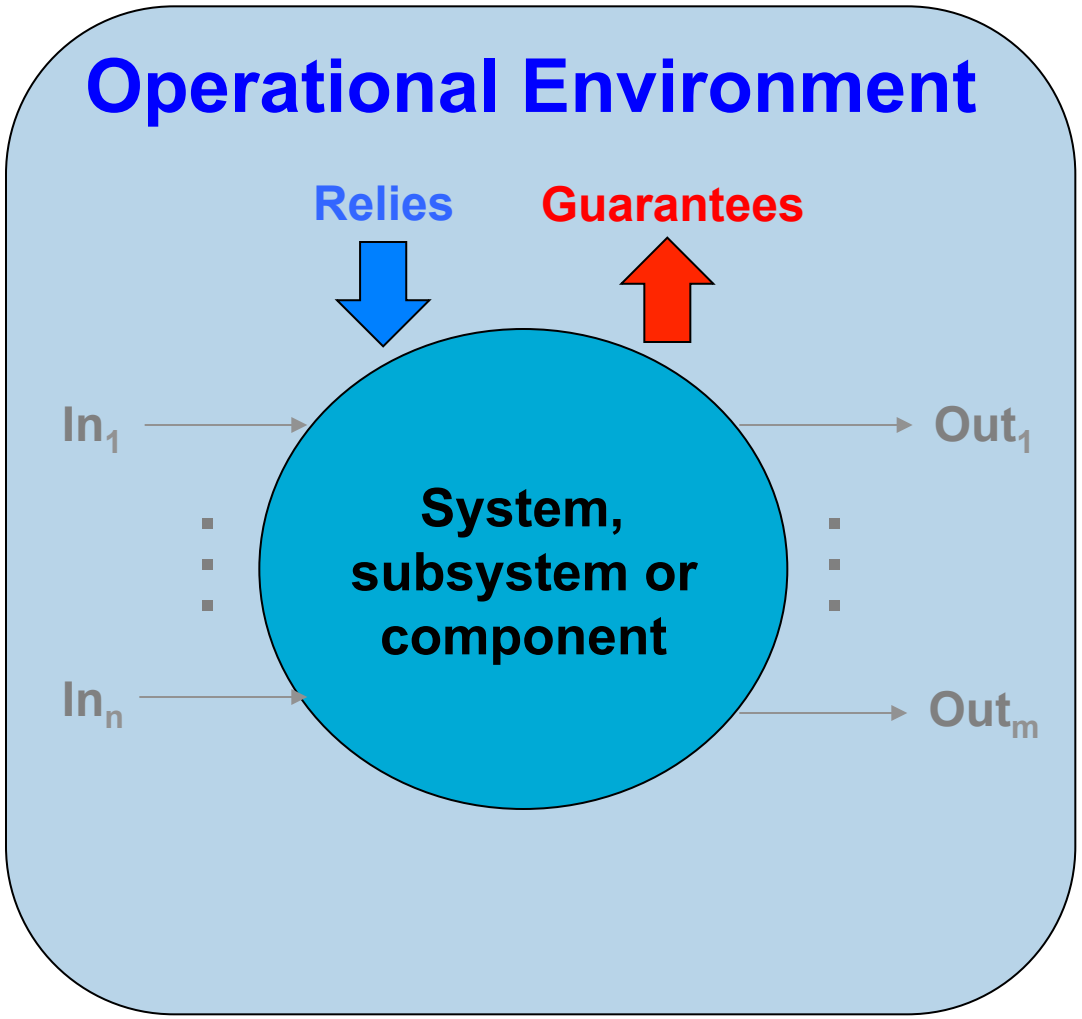
"Boxes and arrows" are a pervasive mode of expression.

*** Source: John Rushby, "Design and Verification of Secure Systems", 1981.**

Inputs and Outputs; Relies and Guarantees

Inputs =
<In_1, … , In_n>
a tuple

***Inputs* =**
trace(Inputs)
(a sequence
of tuples)

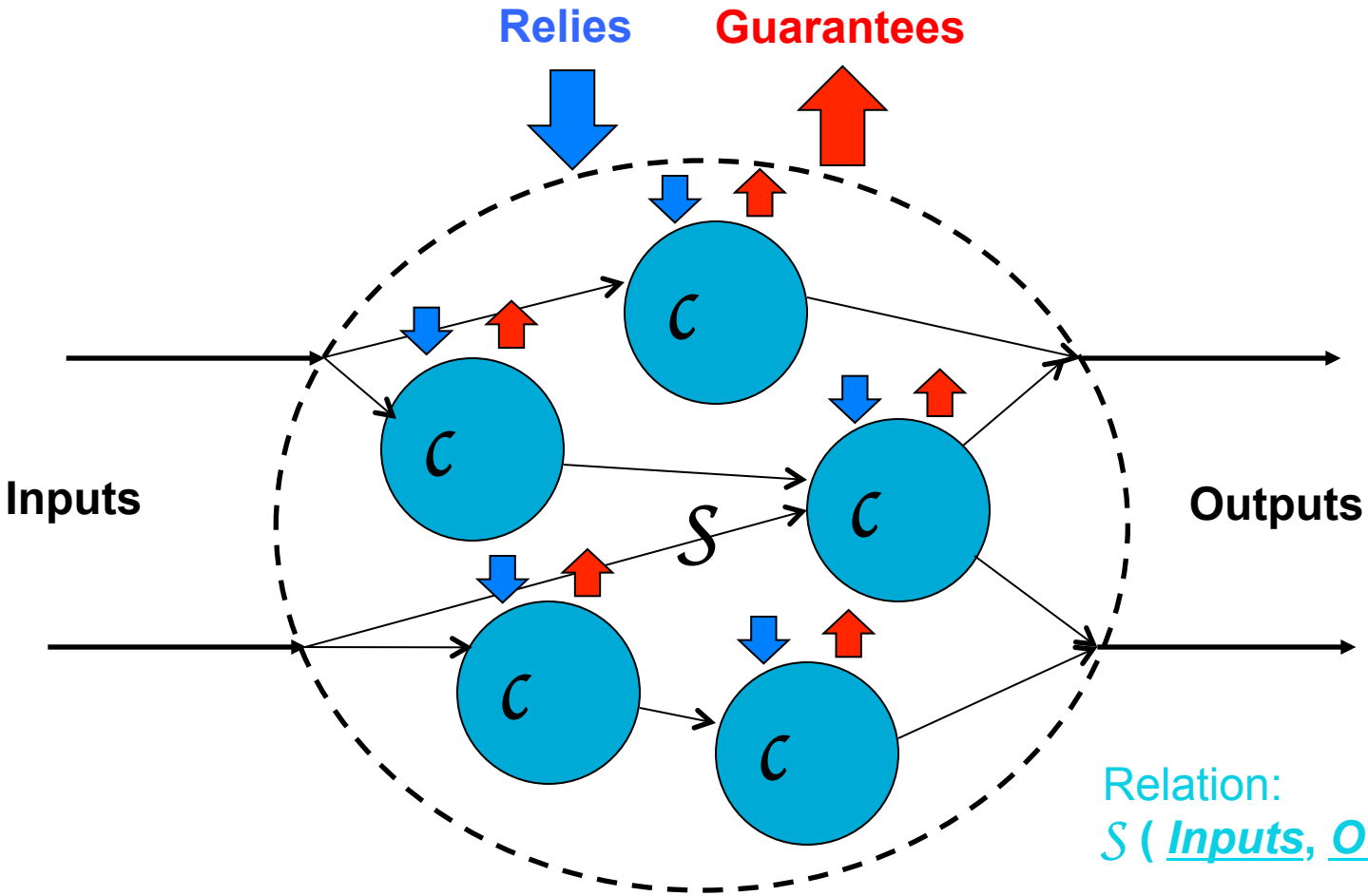


Outputs =
<Out_1, … , Out_m>
a tuple

***Outputs* =**
trace(Outputs)
(a sequence
of tuples)

Behavior $\mathcal{B}$(*Inputs*, *Outputs*) or Property $\mathcal{P}$(*Inputs*, *Outputs*)
are relations on traces, each property defining a set of traces

System $\mathcal{S}$ is made from Components / Subsystems c

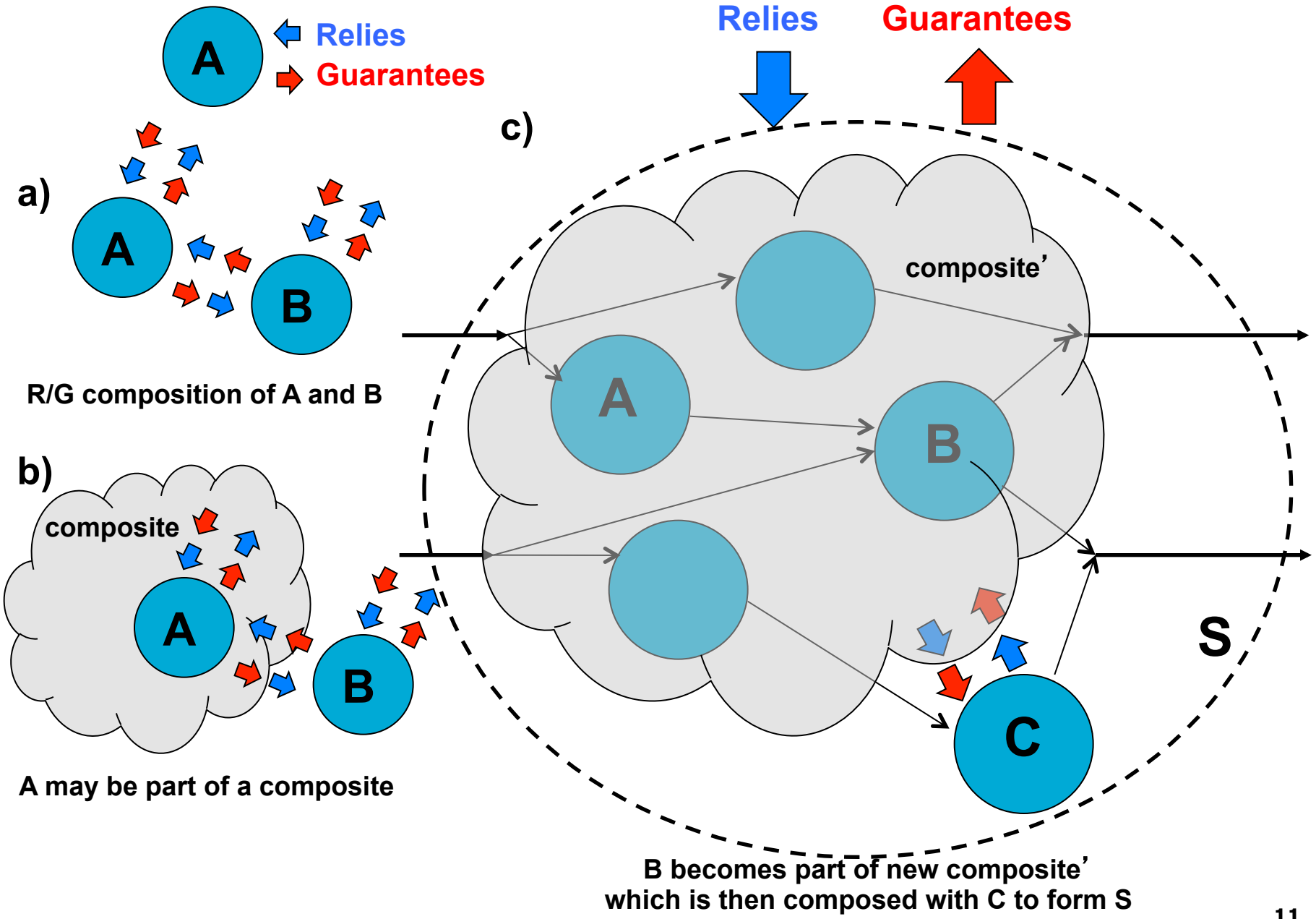


Relies and Guarantees are properties: $\mathcal{P}$ (*Inputs*, *Outputs*)

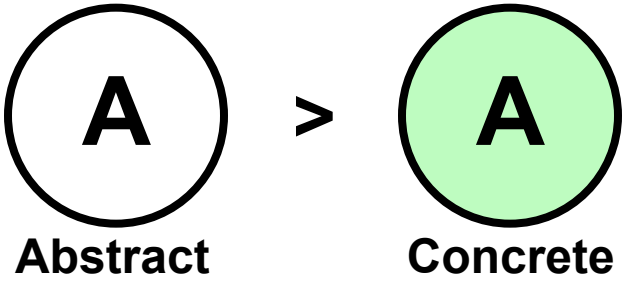
$\mathcal{S}$ satisfies $\mathcal{P}$ if $\mathcal{S}$ is a subset* of $\mathcal{P}$ traces($\mathcal{S}$) a subset of traces ($\mathcal{P}$)

*** More precisely, the sets of traces generated by $\mathcal{S}$ and $\mathcal{P}$**

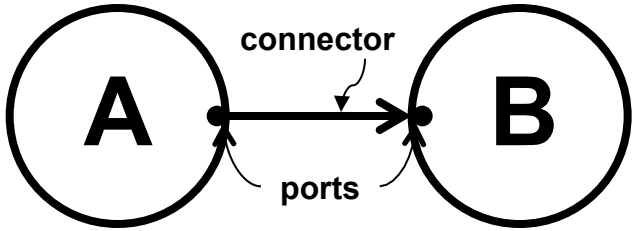
Incremental Rely / Guarantee composition



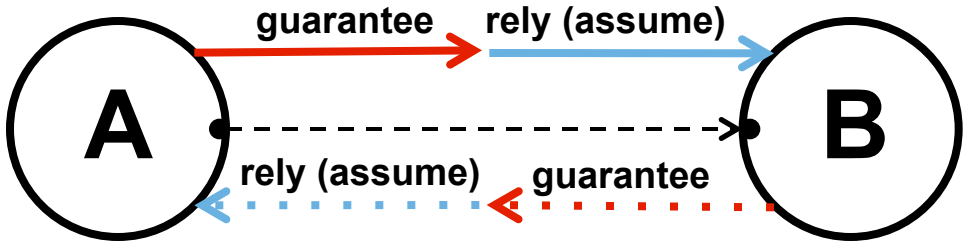
Concrete and abstract components under composition



Abstract and concrete component A (may write as A_A and A_C to distinguish) The concrete component is a *refinement* of the abstract component. The abstract component is greater in the sense that it admits a greater set of behaviors.



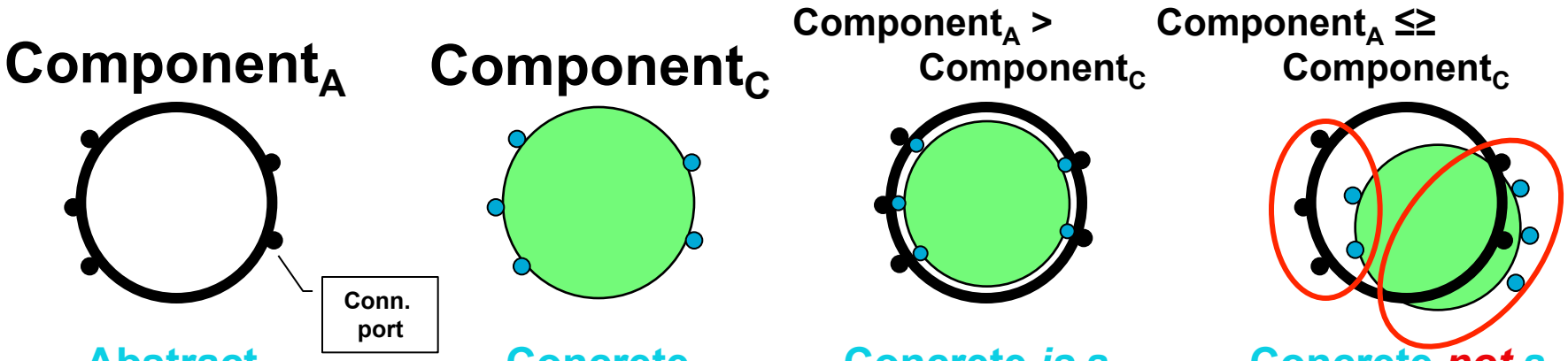
A connector represents an information flow or causality between components



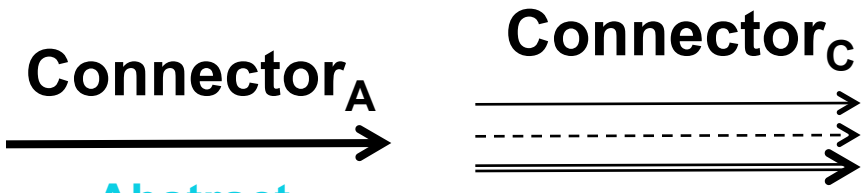
Abstract components may have rely / guarantee relationship

We consider compositions of abstract components and refinements of such compositions that preserve the rely / guarantee relationship

Abstract and concrete policy architecture elements

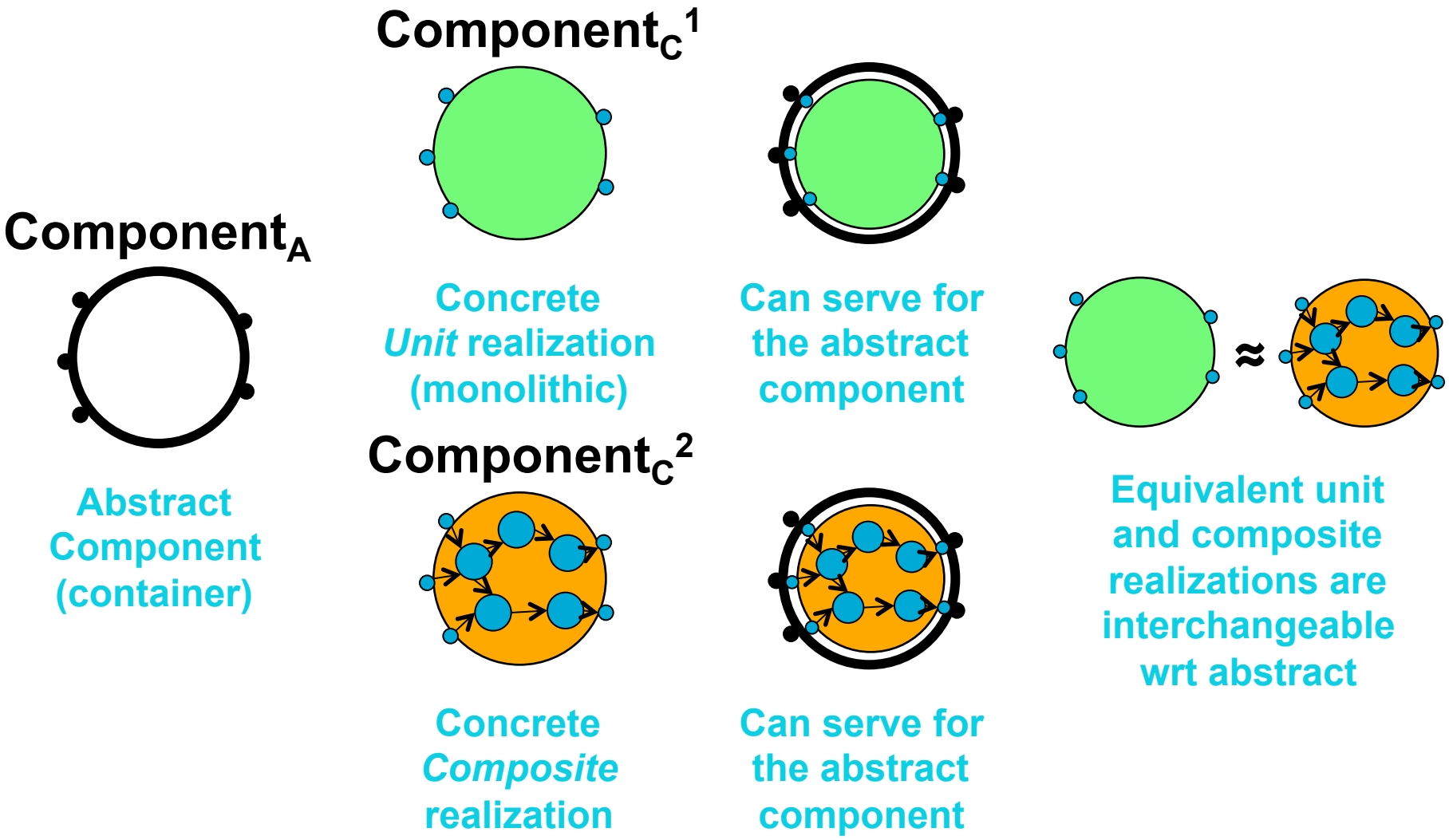


(A refinement may later be further refined)

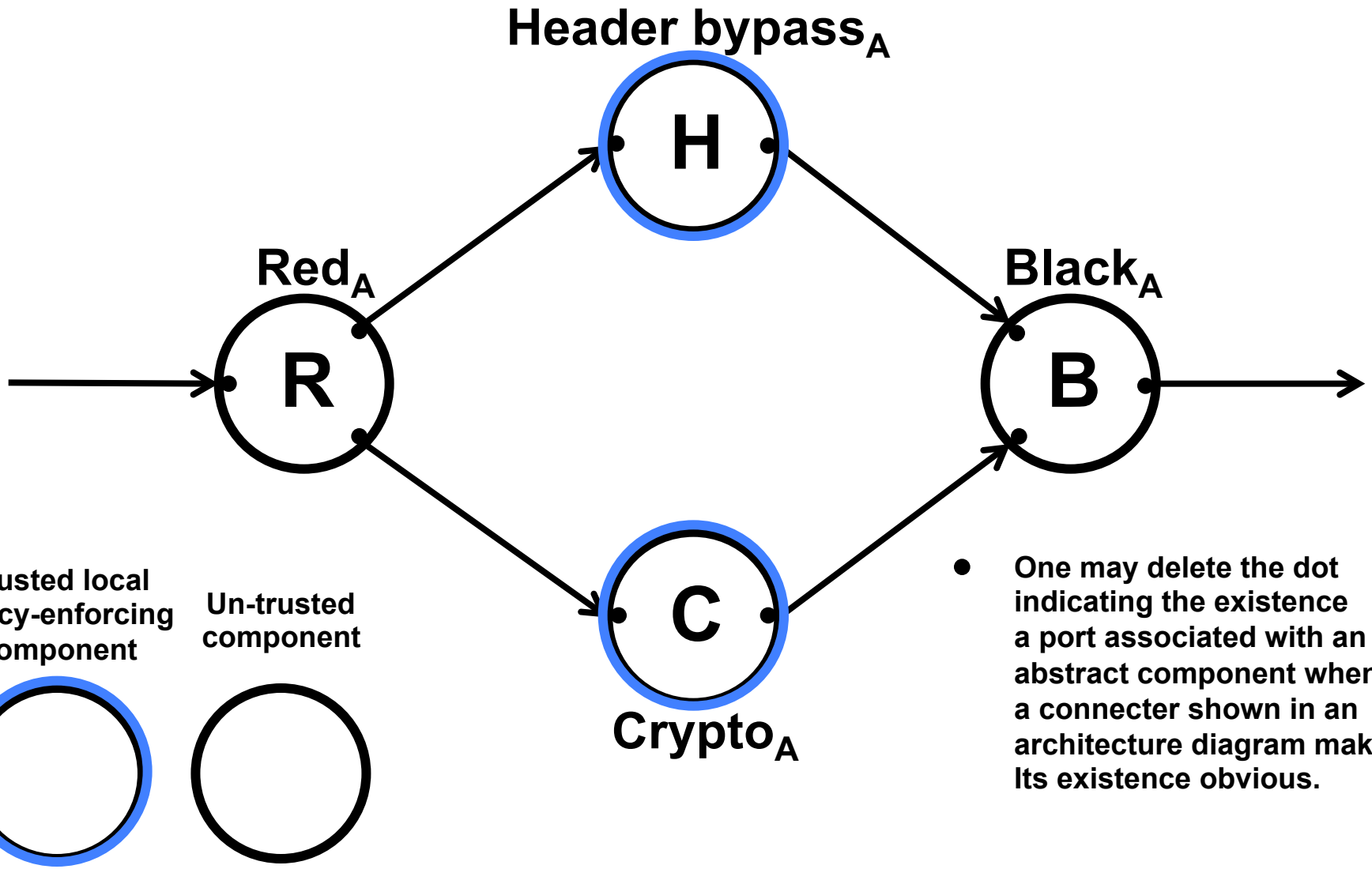


Refinements of abstract connector:
- buffered message passing
- synchronous rendezvous
- shared memory with synch.
- shared memory w/o synch.
- etc.

Abstract components: realized by units or composites

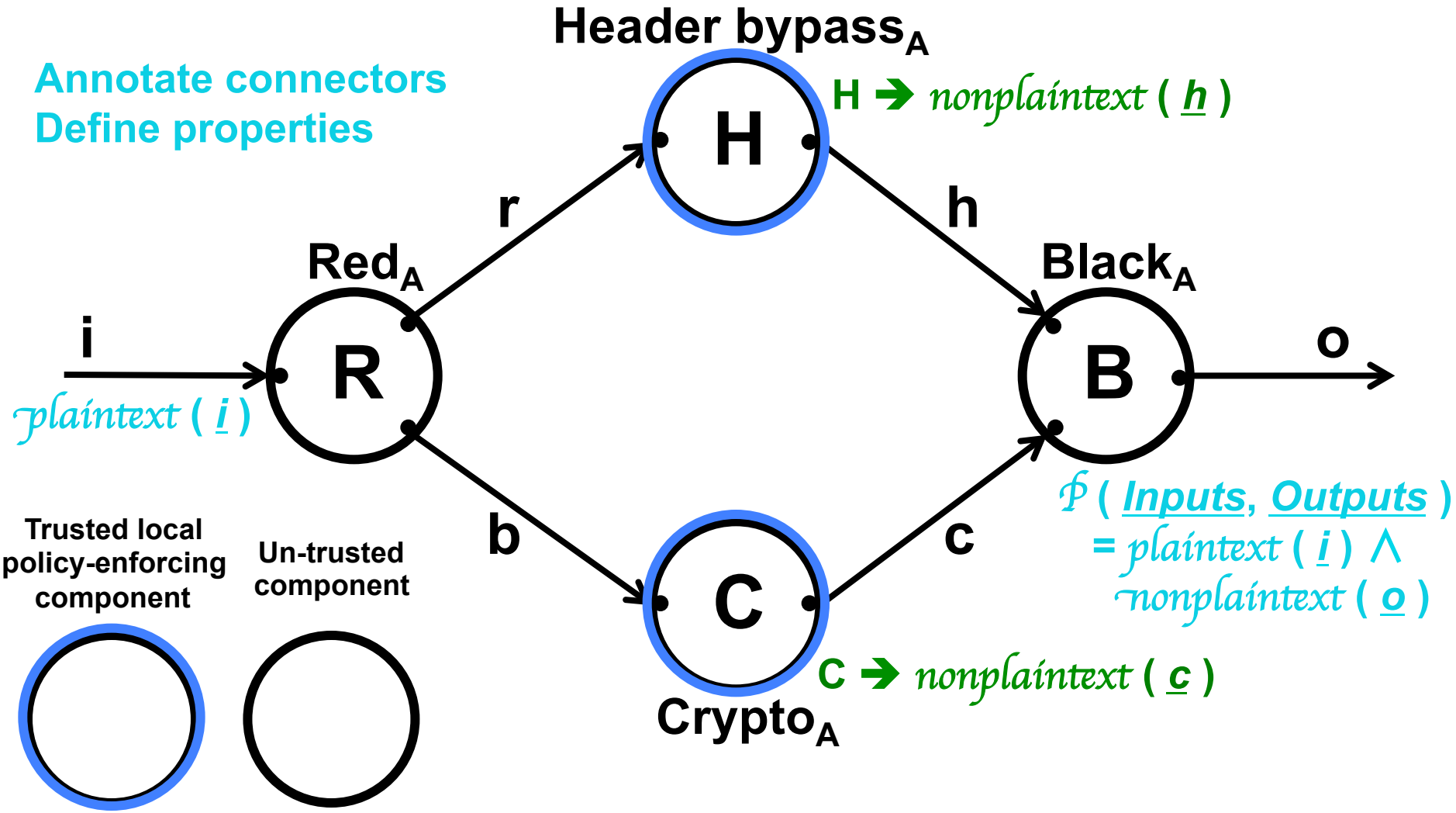


Example: Abstract policy architecture of "Red-Crypto-Black" System

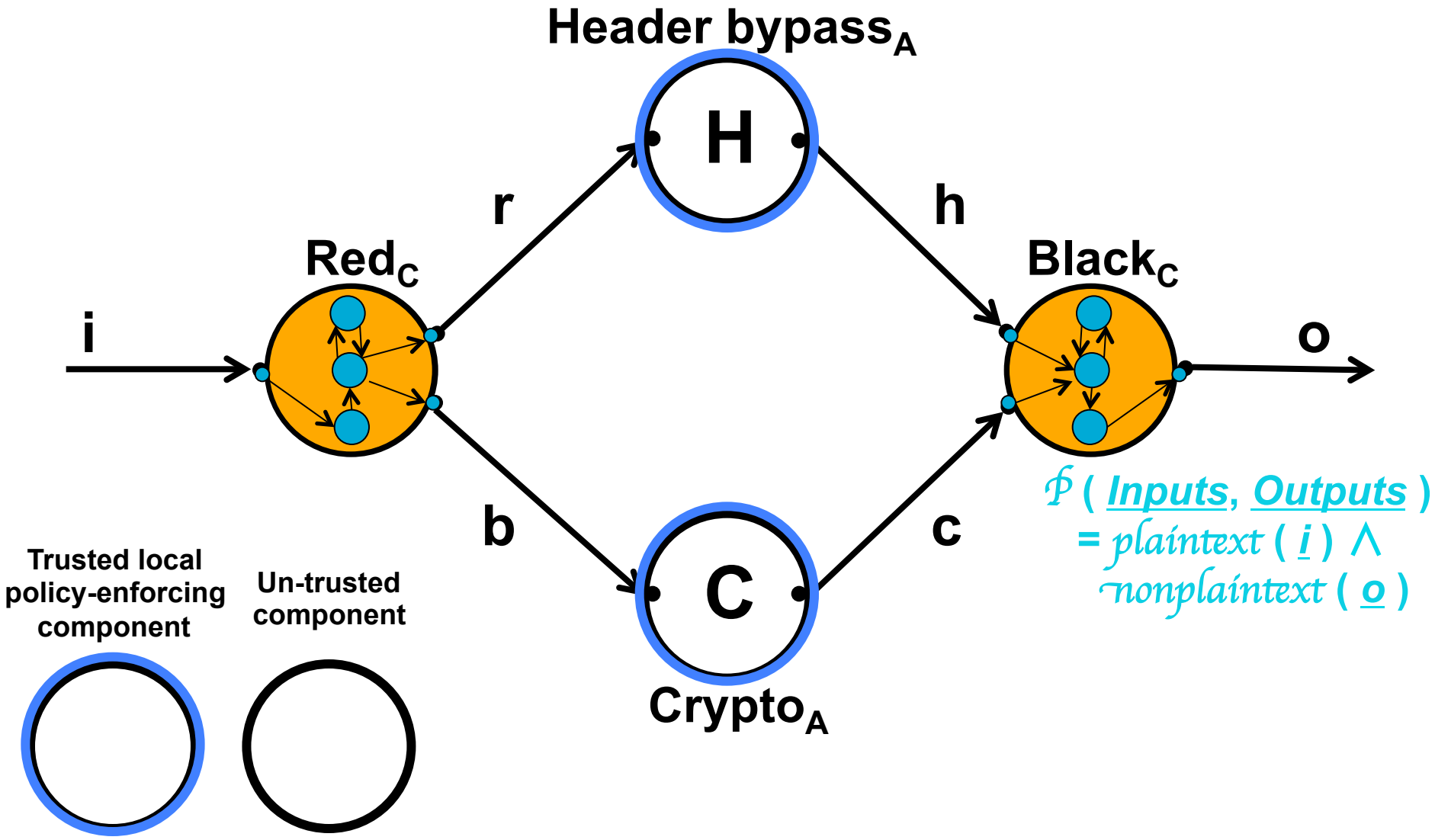


- One may delete the dot indicating the existence a port associated with an abstract component when a connecter shown in an architecture diagram makes Its existence obvious.

Properties required of "Red-Crypto-Black" system established architecturally by relying on properties of components H and C and the form of the composition

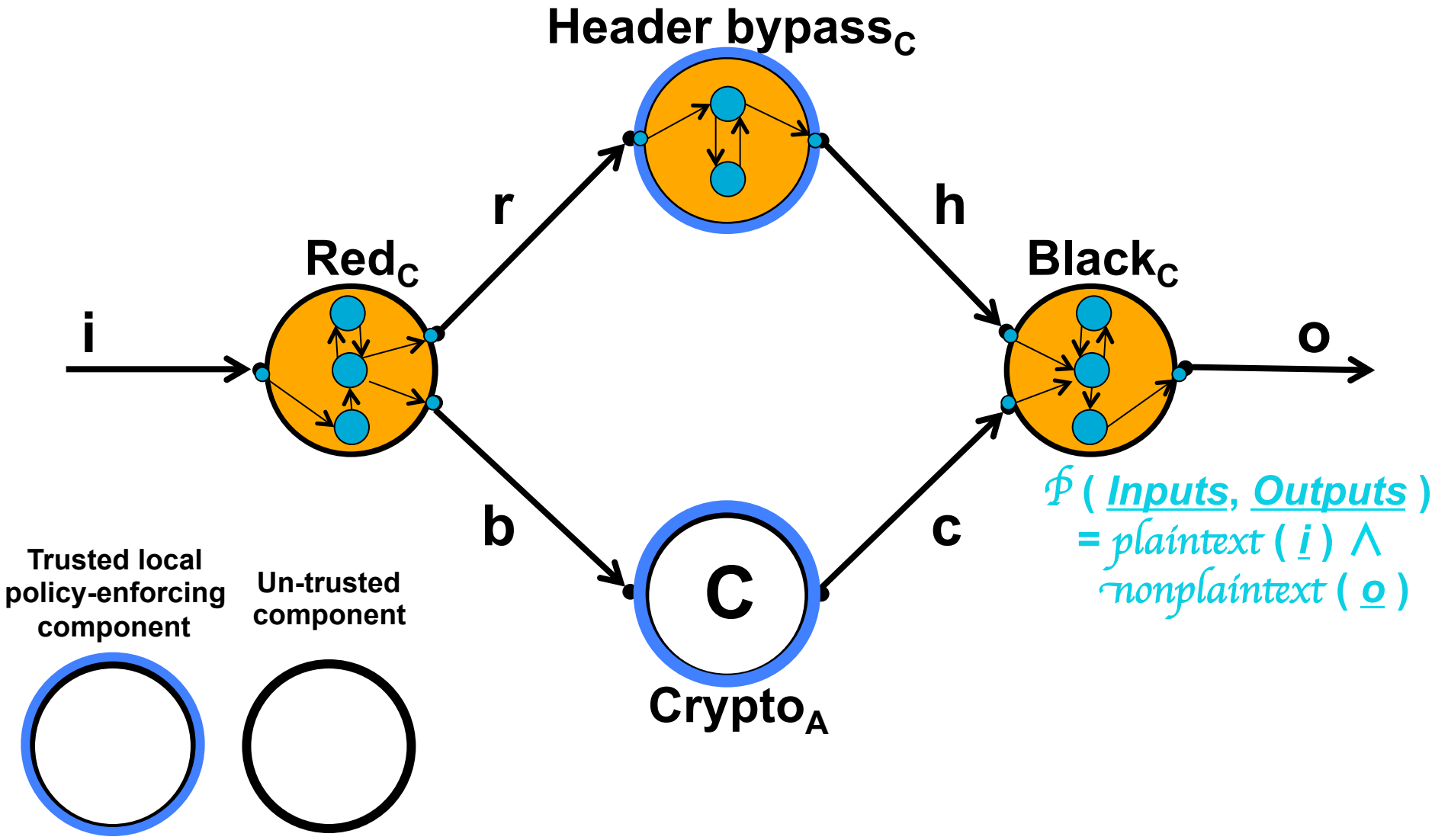


Realization of "Red-Crypto-Black" System, step 1 architecture + un-trusted components refinement

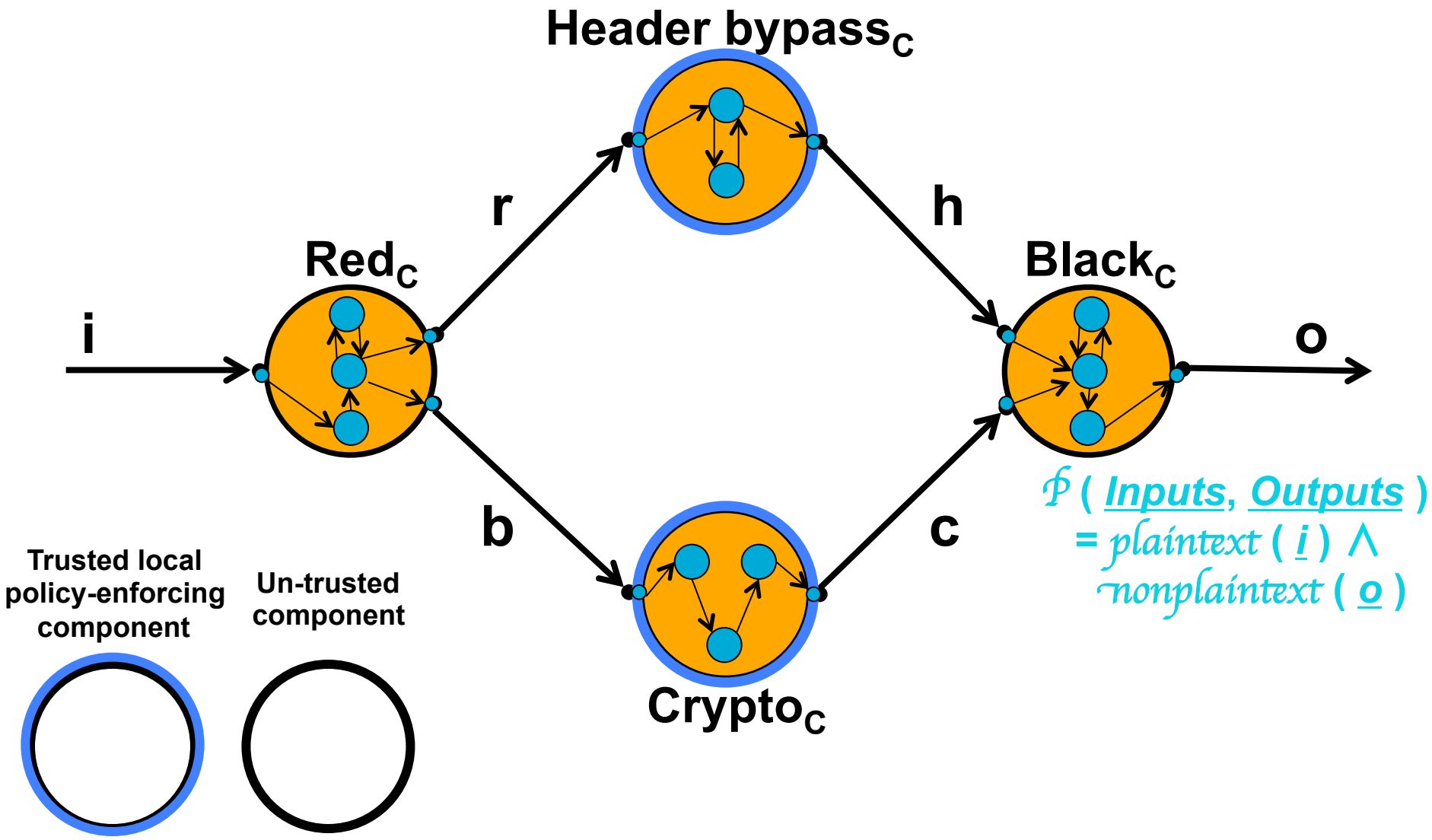


$\mathcal{P}$ (*Inputs*, *Outputs*)
= *plaintext* (*i*) ∧
nonplaintext (*o*)

Realization of "Red-Crypto-Black" System, step 2 policy-enforcing component Header bypass refinement



Realization of "Red-Crypto-Black" System, step 3 policy-enforcing component Crypto refinement



$\mathcal{P}$ (*Inputs*, *Outputs*)
= *plaintext* (*i*) ∧
nonplaintext (*o*)

COMPASS and MILS were a perfect match!

- ***All*** of these aspirations of MILS have now been ***fulfilled*** by COMPASS (as extended in D-MILS)

What about the future of COMPASS and MILS?

- MILS has yet further aspirations:
- E.g. assured:
  - Initialisation
  - Dynamic reconfiguration (beyond modes)
  - Monitoring plane
  - Adaptive behaviour
  - Resilience in unpredictable environments
  - Autonomous behaviour