2001 ISSE INFORMATION SECURITY SOLUTIONS EUROPE

Demystifying international cross-recognition of PKI

We've been barking up the wrong tree!

Stephen Wilson

Director, Policy & Strategy

PricewaterhouseCoopers beTRUSTed

London

The drivers for PKI

Fundamentally, PKI best meets the need to

sign high value or high risk routine transactions

Persistent authentication of a document, not fleeting authentication for access control

Especially non-value transactions
c.f. SET

Because the ROI comes from high volumes with no paper
c.f. Post Office certs

Contracts, records, reports, etc; not access control

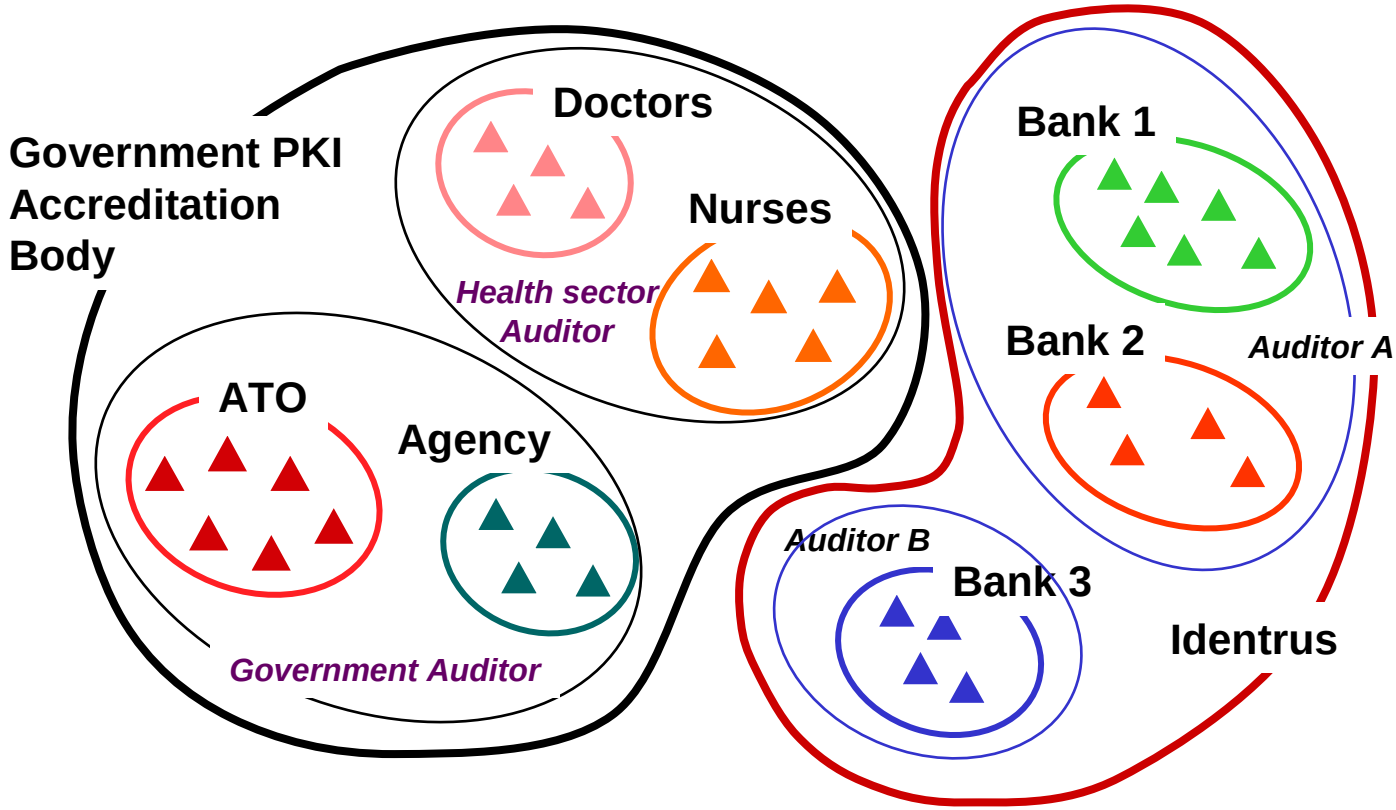
Best practice in PKI

- Government
  - Hong Kong Tradelink (100,000+ certs)
  - Australian Tax Office eBAS (electronic business activity statement; 70,000 small businesses; 1000 new users per month)
  - US Patents & Trademarks Office (target 30,000 patent applications to go online = US$6M saving est. year 1)

Best practice in PKI cont.

- Finance
  - Identrus
  - Australian Project Angus (Commonwealth to cross recognise Identrus member banks)
- Healthcare
  - Australian Health Insurance Commission
  - Australian Electronic Health Records project (see www.health.gov.au/healthonline/ehr_rep.htm)

Community of Interest based PKI



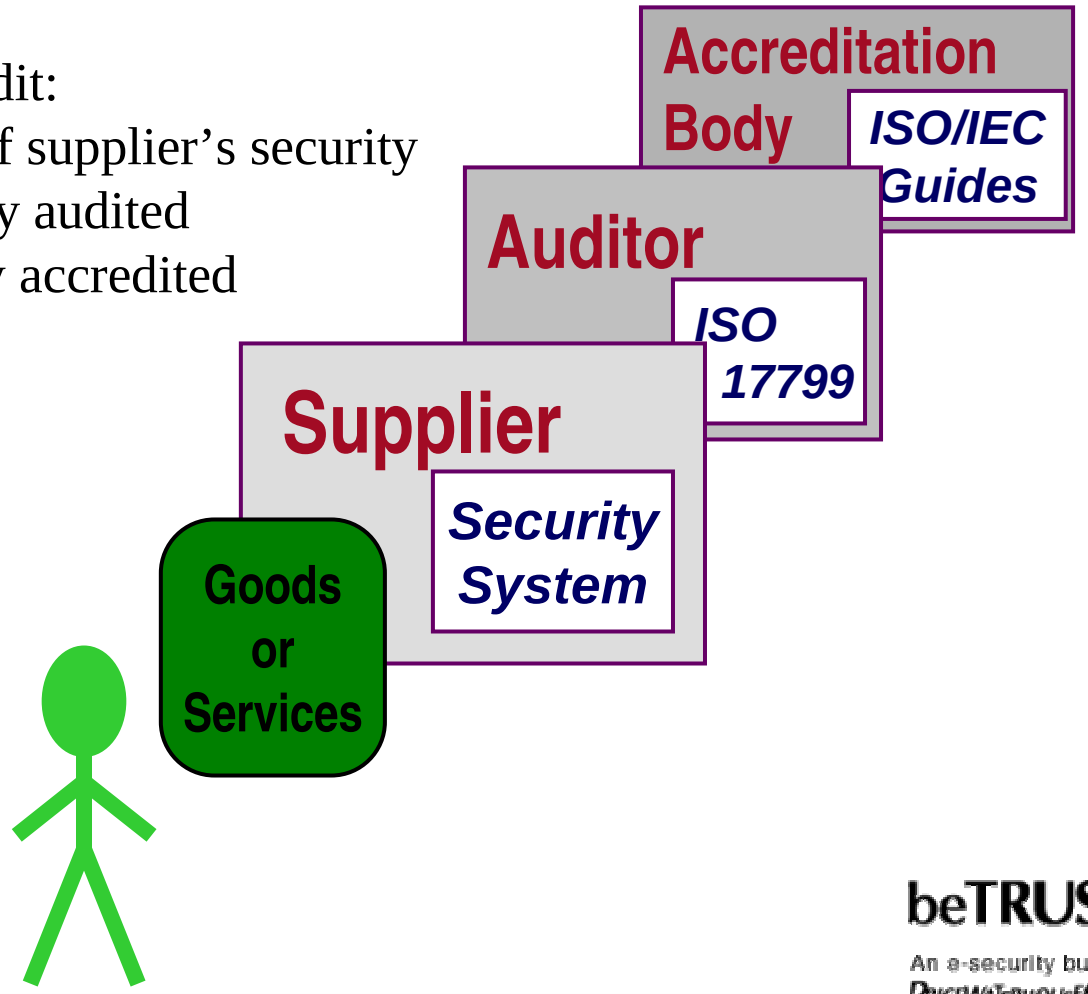
Nests versus trees

- "Hierarchical" PKI tree diagrams historically unpopular
- PKI less threatening when drawn as nested communities!
- Each CA represents a community
- Auditors in turn define communities of compliant CAs
- Mathematically of course it's identical to the tree
- But for regulators and politicians, this is important
- Even for PKI specialists, reveals new ways to think about
  - cross recognition
  - bottom up promulgation of certificate policy
  - multiple root CAs!

Audit based PKI

In a traditional infosec audit:

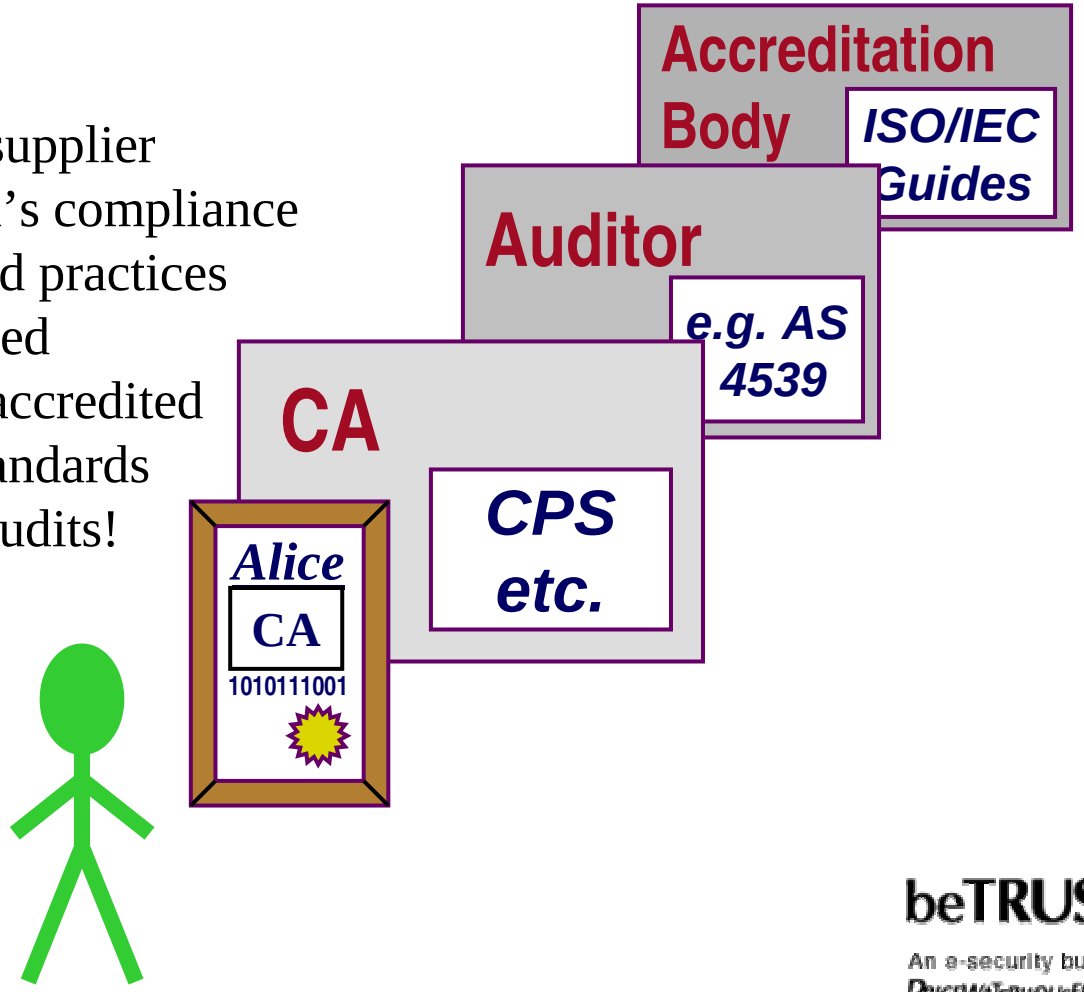
- Buyer seeks assurance of supplier's security
- Supplier is independently audited
- Auditor is independently accredited



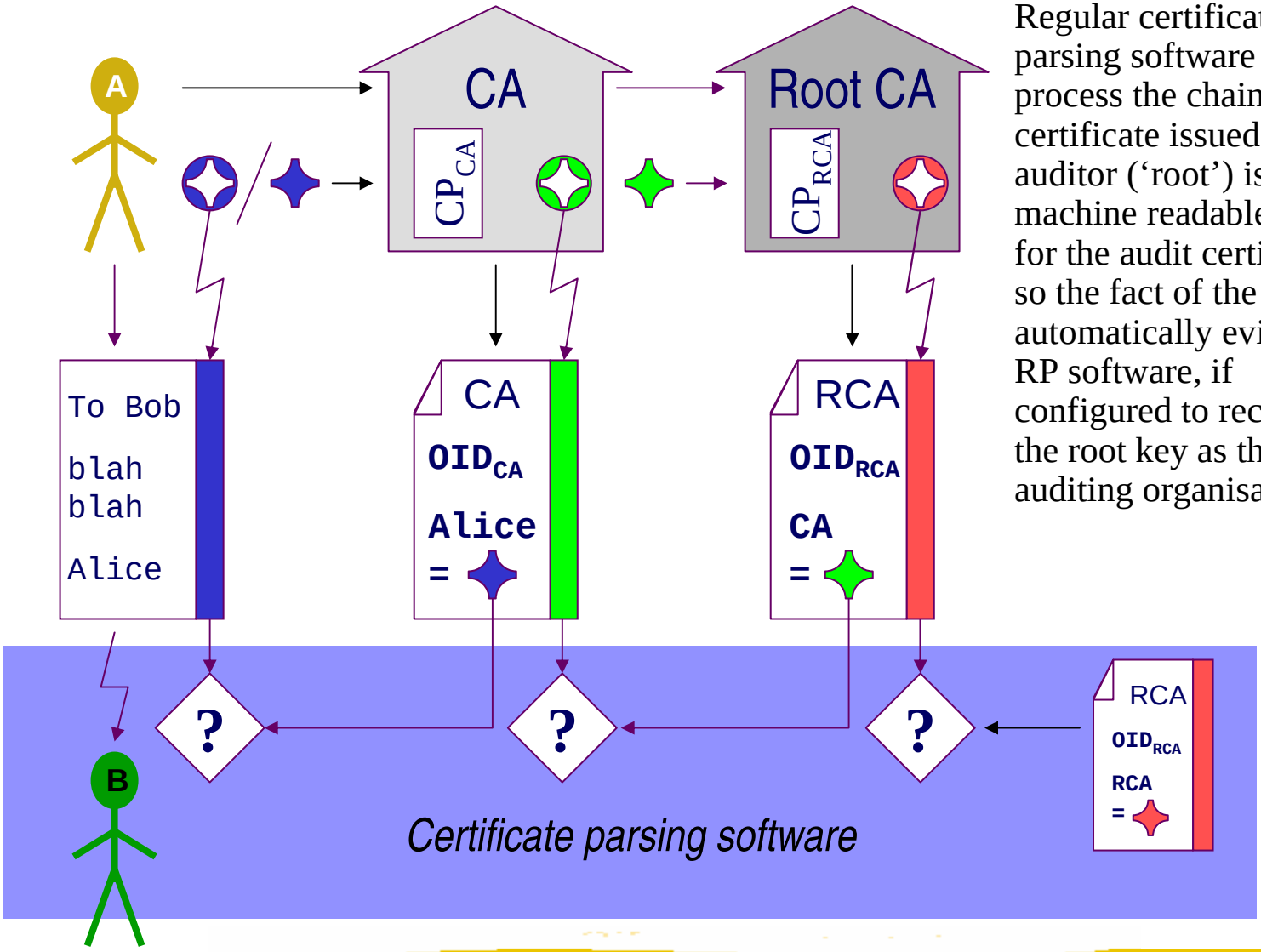
Audit based PKI cont.

It is proposed that in PKI:

- The CA be regarded as a supplier
- RP seeks assurance of CA's compliance with standards & disclosed practices
- CA is independently audited
- Auditor is independently accredited
- The same accreditation standards might apply as for other audits!

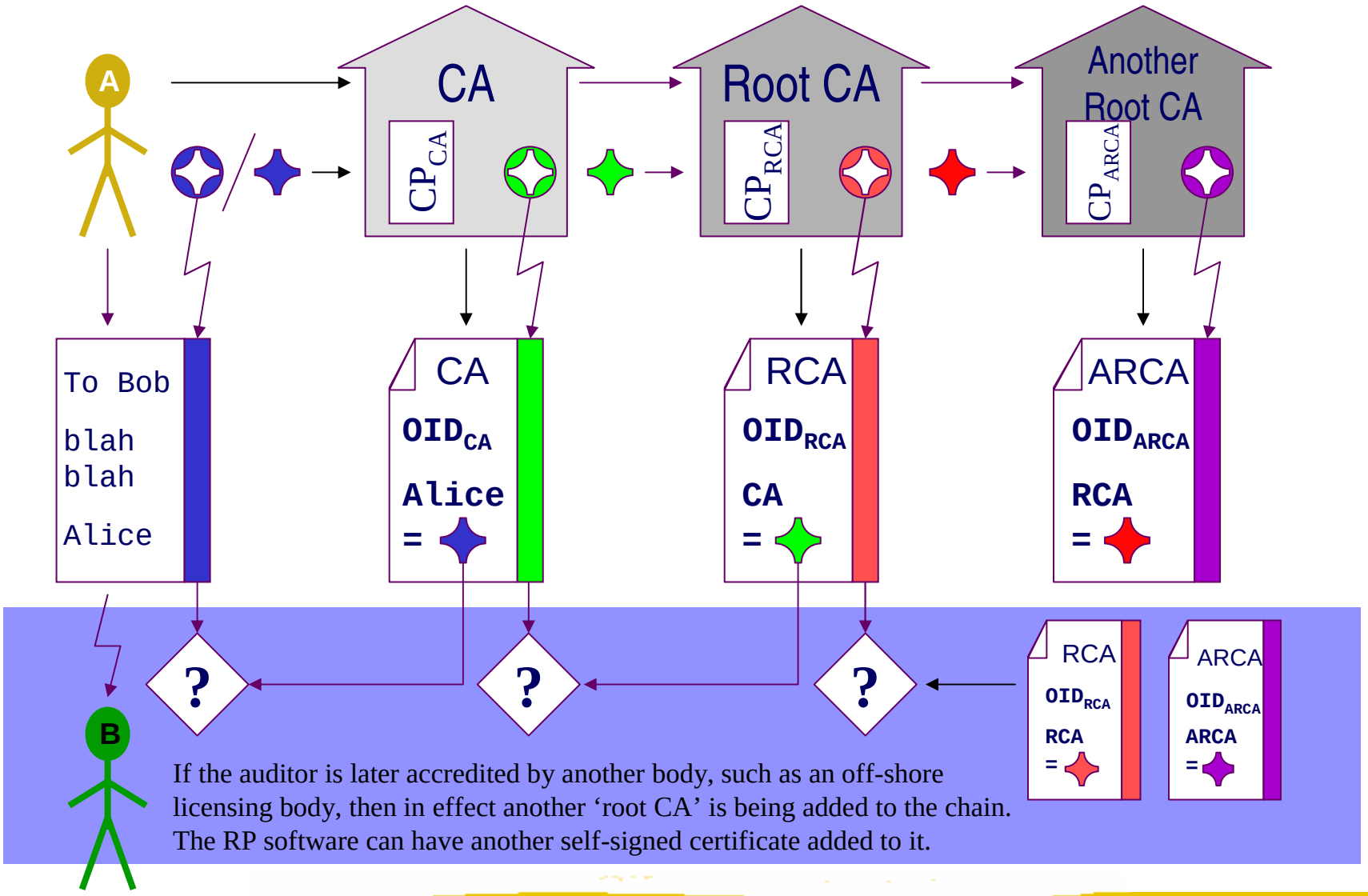


Certificate chains



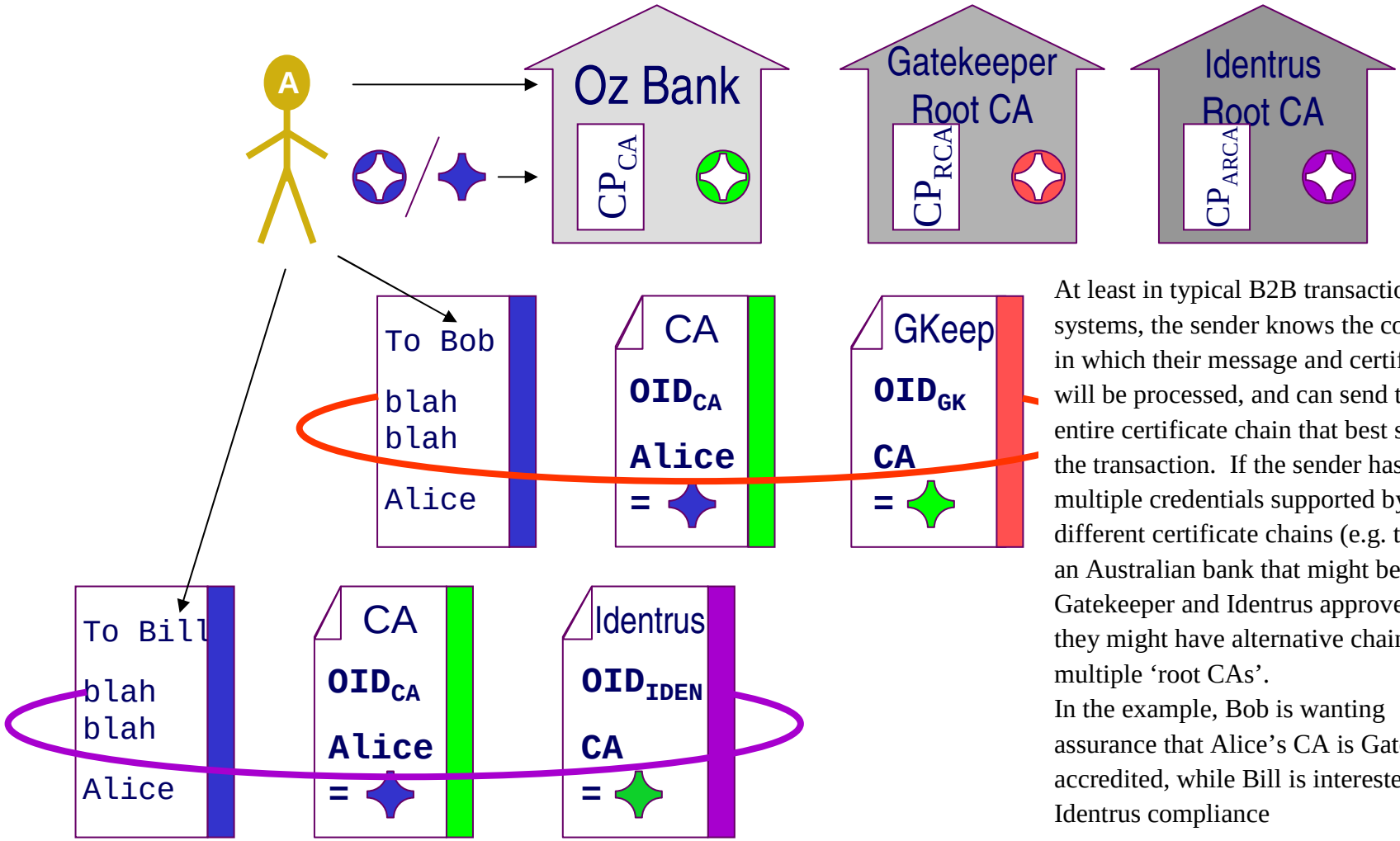
Regular certificate parsing software can process the chain. The certificate issued by the auditor ('root') is a machine readable proxy for the audit certificate, so the fact of the audit is automatically evident to RP software, if configured to recognise the root key as that of an auditing organisation.

Auditing the auditors



If the auditor is later accredited by another body, such as an off-shore licensing body, then in effect another ‘root CA’ is being added to the chain. The RP software can have another self-signed certificate added to it.

The notion of multiple root CAs!



At least in typical B2B transaction systems, the sender knows the context in which their message and certificate will be processed, and can send the entire certificate chain that best supports the transaction. If the sender has multiple credentials supported by different certificate chains (e.g. they are an Australian bank that might be both Gatekeeper and Identrus approved) then they might have alternative chains with multiple 'root CAs'.

In the example, Bob is wanting assurance that Alice's CA is Gatekeeper accredited, while Bill is interested in Identrus compliance

Advantages of audit based PKI

- Light touch; no legislation needed
- Industry-based yet highly trusted
- Utilises existing accreditation bodies & international processes
- Transparent liability for all types of CA
- Demystifies the role of Root CA
- Supports fitness for purpose