A critical look at Bridge CAs

This paper builds on Babystep No. 5 "Clarifying PKI interoperability", looking critically at the Bridge CA model. BCAs might not be ideal in non-government environments.

Recap: What does the receiver need to know?

In Babystep No. 5 we started with the APEC definition of authentication – the means by which a transaction recipient can assess whether to accept or reject that transaction – and found that there are three main things that need to be made known about a certificate:

1. Is the certificate holder still valid (i.e. not revoked)?
2. What representations does it make about its holder?
3. Was the issuer complying with applicable standards?

When sender and receiver are in different domains, the central challenge of PKI interoperability is to be able to deliver these three pieces of information to the systems that need it. Determining validity is nearly trivial, through OCSP or CRLs. But points 2 and 3, which together define *fitness for purpose*, are more complex.

Fitness for purpose

Historically, the fitness of certificates from other domains has been analysed through cross-certification and "policy mapping": an exhaustive comparison of your Certificate Policy (and Certificate Practice Statement) against another's. The desired end result was a *cross-certificate* that causes certificates from other domains to chain back to a local root, as if those certificates were *equivalent* to local ones, imbuing them with the same "trust level".

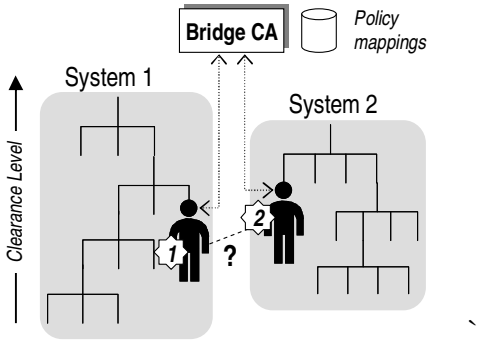
Cross-certification has several problems. It is laborious (so much so that to our knowledge, only once has it ever been completed between two countries). More fundamentally it presupposes that the receiver belongs to a PKI. But clearly there are plenty of digital signature applications where the receiver does not have their own certificate. Finally, the fitness for purpose of a certificate is a different sort of property from "trust level". Digital credentials come in all sorts of shades; it simply doesn't make sense to compare the generic trust level of say a doctor's certificate with that of a lawyer.

Interoperability via a Bridge CA

Before examining the Bridge CA, we should review why the certificate equivalence became so enmeshed in thinking about PKI interoperability.

Governments (especially defence agencies) were the first adopters of PKI. In a typical government PKI, trust levels are much like security clearances. Officials in different domains need to know one another's clearance levels, in order to judge whether classified information can be disclosed by senders or trusted by receivers. So the crucial question was indeed: *Is your trust level equivalent to mine, or is it higher or lower?*

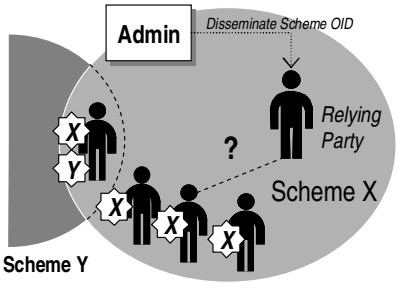
The objective of a Bridge CA, in an environment where multiple CAs would seek cross certification, is to centralise all policy mapping. Instead of all CAs needing to cross-certify in a pair-wise fashion, the aim is that any two given certificates from participating systems can be tested in real time and chained together on the spot if they are deemed equivalent.



Cross recognition in Scheme-based PKI

In contrast to classical government PKI, in a "vertical" or *Scheme-based* PKI, members are issued with credentials for a particular purpose or business application. A trusted scheme administrator vouches for scheme members, issuing certificates with a defined scope, which confer rights to carry out prescribed types of transactions governed by the scheme. The scheme is not necessarily "closed", but all Relying Parties must recognise the authority of the scheme and agree to abide by its rules.

Now the Relying Party's question is much more straightforward: *Does your certificate show that you a legitimate member of a scheme I recognise?*



Unambiguous indication of the scheme to which a certificate belongs – and therefore its fitness for purpose – is coded by the Policy Object ID, which originates from the scheme administrator, and which can be disseminated via regulators and others. Cross-recognition of these types of certificates is automatic if Relying Party software has knowledge of the expected Policy OID(s), via for example a *Certificate Trust List*.