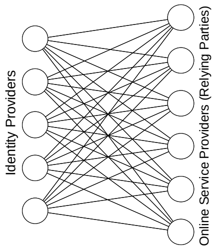
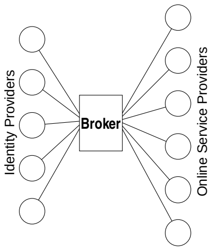
Breaking down identity silos is harder than it looks

Many federated identity models involve a central authentication broker, intended to break down "silos" that hold individuals' assertions. In practice these sorts of schemes have proven much harder to launch than expected. Orthodox explanations for this can blame organisations for being too precious about their customers, or for treating security as a competitive differentiator. This paper looks at a more fundamental challenge in federation that has been overlooked.

The supposed benefit of authentication brokers

In general, an authentication broker is supposed to sit between Identity Providers (e.g. banks that have issued logon tokens) and Service Providers (e.g. e-businesses and government agencies) so as to streamline a large number of bilateral relationships. The core idea is that if a user has gone to the trouble of obtaining a credential with one IP, then they ought to be able to use it at multiple participating SPs.





In the diagram above, each link joining service and identity providers represents a legal arrangement. Introducing the broker looks like it reduces the total overhead. But the right hand side is only less expensive overall if the arrangements before and after are comparable.

The re-use of credentials

Re-using an existing credential outside the silo in which it was issued is more complex than it may seem. The classic IPs today issue credentials to their customers for well defined applications, like Internet banking, and do not contemplate the use of those credentials elsewhere. When e.g. One Time Password generators are issued by a bank, typical Ts&Cs forbid their use in other settings. This conservative stance is understandable, especially since most credential issuers wouldn't regard themselves as providing "identities".

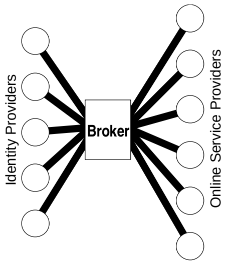
So, if existing credentials are to be re-used in a federation, then the Ts&Cs to which everyone previously signed up will need to be modified, then accepted afresh by customers. Special new contracts will be needed between providers and the authentication broker, to enable existing credentials to be used in new ways.

Lawyer up!

The deep problem with the necessary new contracts is that they sit in an entirely novel environment. The possibility—nay, *promise*—that new SPs will continually join the federation means that IPs must agree to their credentials being used in unexpected applications. The authentication broker will have to draft pro forma contracts with IPs and SPs that somehow circumscribe risks of the unknown. When providers that want to join up engage their lawyers to review these unprecedented contracts, what will they make of them? For starters they will want to know how liability is to be managed if an error made by one IP can damage untold SPs.

Identity federation takes carefully crafted contractual silos, in which businesses know their customers for the purposes of specific applications, and breaks them open so that strangers with no prior relationship can transact with those customers. The cost of having lawyers even come to grips with this situation, let alone negotiate around the novel pro forma contracts, is huge and difficult to constrain. This is quite unlike a regular service contract negotiation, where the norms and underlying business models are tried and tested.

Therefore, the diagram at right is a fairer depiction of life after federation. The arrangements between the broker and each player are far more complicated than any existing siloed bilateral relationships.



We should not be surprised that authentication brokers have been difficult to establish—for it turns out that the total cost of a large number of traditional simple contracts is likely less than that of a smaller number of much more complex ones.