



## An authentication family tree

A bewildering array of authenticators is on the market today. How do we make sense of them all? Most people are familiar with single factor versus two factor, but this simple split doesn't help match technologies to applications. The reality is more complex, resembling a "family tree" which branches at various points.

The main split is between *Transient* authentication (i.e. access control) which tells if a user is allowed to get at a resource or not, and *Persistent* authentication, which lets a user to leave a lasting mark (or signature) on what they do, such as binding electronic transactions.

Working our way up the Transient branch, we see that most access controls are based either on *shared secrets* or *biometrics*. Dynamic shared secrets change with every session, either in a series of one time passwords or via challenge-response. Some biometric traits can be left behind inadvertently in the environment and are more readily stolen; we call these "dirty". Others are "clean", leaving no residue. Note that all shared secret methods have been proven to be susceptible to Man-in-the-Middle attack and should be phased out in remote authentication

For persistent authentication, the only practical option today is PKI, which is available in an increasingly wide range of forms. Embedded "hard" certificates are commonplace in smartcards, cell phones, and other devices.

The family tree also shows which technologies in Lockstep's view will continue to thrive, and which seem more likely to be dead-ends.

