An Adaptive Approach
In trading networks such as supply chains in which orders may pass from one office to another, an initial transaction (e.g. an order for an aircraft engine) may spawn multiple supporting transactions (orders to individual parts, orders for shipping containers and so on.) This would involve handling of high volumes of traffic. Business processes that require a mixture of long-running and short-running transactions would require further customization of security.

Requirements for human users can vary. For e.g. customers of an online bookseller would not take on the burden of digital signatures in order to securely order books but bookstore owners would be interested in PKI to protect financial data transactions. Non-repudiation would also be an important aspect in such transactions. The goal should be to apply only as much security as a particular transaction requires, rather than increasing infrastructure costs and applying stringent security measures uniformly to every node and transaction.

An example that illustrates the natural need for an adaptive approach to implementing security is the decision of most companies to postpone the use of Digital signatures as The cost for implementing a PKI infrastructure is very high.

Thus for simple Web services having one to one or one to many applications, the existing security mechanisms in Web services do suffice, but when it comes to sophisticated Web services involving long running transactions that traverse multiple enterprise boundaries there is a need to protect messages persistently. Security measures like XML encryption and Digital Signatures work well for such enterprises but at the same time a trust model with a third party credentialing may be desirable.