In order to deliver a valuable service in Peer-to-Peer (P2P) applications, it is important that participants act correctly. In an open and heterogeneous P2P environment, services have to contend with malicious and selfish nodes. Trust is essential to encourage cooperation and the improvement of the quality of service a peer provides. This thesis studies solutions to provide the substrate to build trustworthy applications in P2P networks. Peer-to-Peer (P2P) networks are very attractive to build large scale applications. The fully distributed nature of P2P networks creates a scalable, fault tolerant and self-organized system with the potential to involve millions of nodes. In the presence of untrusted nodes, the robustness and performance of Peer-to-Peer applications is degraded. In an open environment, such as Internet, users from all parts of the world interact and share their resources without knowing each other. Untrusted nodes in the network may be faulty, malicious and selfish, or even act together to attack the application. Different approaches have been presented to build trustworthy applications, some of them do not scale or assume trusted peers that are not always available in P2P networks. Others, use specialized hardware or are focused in detecting malicious peers, not taking into account that identities in P2P networks are cheap and a malicious node can re-enter the system with a new identity without problem. In this case the detection mechanisms only solve momentarily the problem. This thesis contributes to build trustworthy applications in large scale distributed networks: 1. We analyse the components and vulnerabilities of distributed reputation systems in large scale, distributed networks. 2. We propose a reputation system that introduces the concept of risk to mitigate malicious attacks. 3. We propose a membership algorithm to build a scalable pseudo-trusted ring within a DHT that can provide trustworthy services in a P2P network. CORPS builds trust using a reputation system to decide whether a node can be a member of the community or not. 4. We use CORPS to put together a reliable routing P2P service over DHTs. An evaluation of the probability of failure for this trusted service is given.