card space, due to the lucrative potential afforded by fraud, identify theft and all that this entails, a smart card must also embody trust technology if it is to be truly considered a TPD. This implies that the dependency of smart cards on the perceived trustworthiness of public host machines, to which they interface, should be eliminated and that security, based only on cryptography and SSL/TLS technology, needs to be augmented with trust technologies and protocols. In addition, the security solutions based on USB smart card [26], [27], [28] still need some software (i.e. Host Agent) to run in the host machines to proxy the communication between the smart cards and the remote servers. On the one hand, if the host is untrusted, it is hard to guarantee the integrity of such proxy software. On the other hand, if the smart card is not trusted by the host owners, the proxy software might not be allowed to run.

To satisfy these requirements, an alternative breed of TPD is emerging that specifically addresses the problem of creating a trusted environment on an untrusted host using a combination of a TPM to establish a root-of-trust and virtualization technology supporting virtual machines that can provide well supported, strong isolation between applications. As network smart cards and this emerging breed of TPD evolve, utilizing similar technologies and form factors (e.g. USB token), the technical distinction between them will become increasingly blurred. As such the dominant distinguishing factor between these two classes of device will no doubt be the application scenarios of use. We next focus on the emerging breed of TPD relevant to our paper.

As part of its Securing the Intelligent Nation initiative, the Singaporean government has introduced a standardized nationwide security smart token called Digital Online Registration and Identification System (DORIS) [29]. This token offers all Singaporean companies and citizens certified, secure access to government services. DORIS is implemented as a specialised USB thumb-drive hardware token. The core of DORIS is a secure microcontroller, flash memory, and a small radio transceiver and antenna used for electronic ID and online/offline authentication.

DORIS suffers from a portability and mobility problem as it requires an installation of a specific driver. To address this problem, a software version of the device was developed, called Dynamic Isolation of Virtualized Applications (DIVA) [17]. When DIVA is plugged into a PC, it creates an isolated command window which acts as a user’s own trusted software execution space to provide secure access to a wide variety of applications. Furthermore, the user interacts with the virtual application via a Virtual Keyboard to mitigate the risk of key stroke logging attacks. One of the limitations of DIVA is that it can only be used on the Windows platform, as it was built specifically for that environment. Furthermore, DIVA is a pure software based solution as compared to its predecessor DORIS. We have also developed a similar prototype system based on TCG specification, called Trust Extension Device (TED) [30]. It uses the type II virtual machine and emulated TPM. Though it provides a seamless portability and mobility, it cannot provide the isolated execution space due to the inherent limitations of type II virtual machine.

In addition to the government services, the need of a mobile and portable trusted environment is realised in other application domains including enterprise applications. In recent times, a number of commercial products have emerged for enterprise applications. Encryptakey is a small portable (USB form factor) device that allows mobile users to create a seamless and secure environment in which one can perform digital transactions, surf the Web, conduct business and communicate securely and privately [10]. Encryptakey is a biometrically authenticated device which offers multiple-levels of authentication and comprises its