Abstract

Web technology is propagating at a high speed to every corner of the society’s services, and commerce is one of the services that suffered the biggest impact. E-commerce is a combination of traditional business with improvements from the Internet and information technologies. A particular kind of traditional business where e-commerce may be beneficial is store commerce, where there is a great improvement potential in ecologic, logistic and safety behaviors. An important aspect of the shopping experience is the receipt that is given to customers.

The problem that this thesis is trying to solve is the absence of a system that supports local digital receipt transactions. The major contribution of this thesis is the analysis and design of a client-store communication architecture which supports these transactions, and in particular that supports locally and securely sending the client’s tax identification number to the store and getting back a digital receipt issued to the client that is digitally signed by the store, validated by the client, and that could be used in the client’s tax statement.

To evaluate this architecture, a prototype of a local digital receipt transaction system that abides to the architecture was developed. This thesis describes how this prototype was built using available technologies and tools; digital certificate and secure sockets layer technologies were critical in this development. The prototype implementation validated basic requirements of the architecture that were identified beforehand. An important observation that arises from the experience of developing such a prototype is the lack of compatibility of different technologies on the client’s mobile device and the store’s fixed device.

This is an important starting point for studying similar systems behavior and their limitations and for future research into e.g. creating a cost model of the deployment of such a system.

This thesis also opens the door to debate several privacy issues concerning e.g. both parties’ tax statement data crossing.