Abstract - In this paper we present a framework for boosting trust in discovery of business people, services and pervasive objects for emerging mobile based dynamic business environments. Our approach is based on (i) using authentic discovery URIs and verification methods that can be achieved using digital signatures, followed by (ii) negotiation of micro-policies describing data practices that services promise to deliver. Negotiations are realized through (iii) user-agent assisted evaluation of suitability of micro-policies.

Keywords: Secure discovery; policy negotiation; QR codes.

1 Introduction

The business landscape is changing and today business people often use their smart phones in both personal and business contexts. Often the devices are used to discover and initiate interaction with other business people, network connected physical objects, location specific services and social business communities (see [1]). These micro-interactions (see [2]) are often performed in an ad-hoc manner: either using NFC tags, QR codes or other similar technologies that use URIs to redirect user to particular service. The outcome of such micro-interactions is often that certain apps get installed to the smart phone of the user and later in the process these apps are consequently granted rights to certain part of the user’s subsystem. This may pose a threat to both the business user and the organization he is working for as it may lead to personal and corporate information leaks.

2 Trust Related Requirements

Authentic discovery URIs: URIs stored in discovery mechanisms (such as NFC tags or QR codes) need to be authentic. Additionally it needs to be clear which party has produced the discovery URI and which party is behind redirecting the user to particular service.

Transparency of service provider: When the user is redirected to the location based service, physical object, business community or a business user acting on behalf of another company (from here on all these will be related to as service) it needs to be clear which entity is behind the service. This information needs to be authentic.

Authentic transparent policies and agreements: the party providing a service needs to transparently present the practices to the user. The information on how the service will handle user’s data is negotiated and at the end of the negotiation process both parties should be holding the same signed agreement.

Usability: Although the process of matching service policies to user preferences may be complex it is necessary for software agent on smart phone to automate it to minimize required interaction with the user.

3 Boosting Trust in Service Initiation

3.1 Authentic Discovery of physical objects services

As a solution for the requirements described we propose a framework that allows for i) authentic discovery and for ii.) trusted authentic service initiation. The authentic discovery mechanisms relate to digitally signed redirection URIs, which are deployed through discovery mechanisms, such as NFC tags, QR codes and similar. Conceptually the solution is simple: URI, its digital signature and information about party that signed the URI (such as certificate containing public key) is embedded into the payload space. However, due to the limited storage space available on the tags and QR codes, the actual implementation is not trivial to achieve (see Fig. 1 for details). Other similar approaches that relate to authenticity of QR codes and NFC technology are found in [3]

![Figure 1: Secure QR code structure](image)

3.2 Policy Negotiation or Policy Selection

Formal policies are used to legally define relationship between the parties and to specify conditions under which a service or a community membership is provided by one party (the provider) and consumed by the other party (the requester). This is especially important in dynamic environments where the provider’s policy may have internal rules that are incompatible with requester’s company’s policies ([4], [5]).

To minimize number of network transfers, a 3-step policy selection process is developed as shown in Fig. 2. Each step is secured using digital signatures. In first step, the requester fetches provider’s XML document with multiple alternatives for the policy. Because the policy options are signed by a verifiable identity, the requester can trust the offer is real and the provider will not only collect the requests, possibly associate them with requester’s data like his identity, and then not even provide the advertised service or membership. X.509 [6] certificates and XML-DSig [7] are used in the prototype.
3.3 User Agent

The mobile phone user agent is intended to be a semi-automatic helper tool. It evaluates policies and matches them to preferences of the user (see [9]). The user agent provides assisted service initiation / negotiation dialog that contains visual indicators determining suitability of different options under which the service can be provided. (see Fig. 3)

4 Conclusions

A secure discovery and trustworthy policy negotiation framework and its user agent were presented. The negotiation process and its implementation are simplified to be used on smart phones and the user selects the policy in a single step. This approach still addresses the needs of most providers in the real world. By using digital certificates and signatures, it assures policy consistency during the negotiation process.

5 References