Topic: Enhancing privacy in token based electronic identity schemes.

Introduction

Our proposition for a subject for discussion is based on the fact that a number of hardware tokens will, and already do, include biometrics for end user verification as part of the process of authentication with the token. We also find that in order for hardware based multi factor authentication to penetrate the mass market it will have to provide positive differentiation from the current authentication paradigm through superior user experience and ease of use. Biometrics at this time appears as the most attractive and indeed the most marketed means of creating a positive user experience.

Thus we see that the need to integrate biometrics into any future infrastructure of token based authentication over the web is already established, and so suggest that what is now required is to quantify and understand its impacts on security and privacy, not in a comparison to passwords and PINs but in its own right, and to be able to communicate the quality of end user verification afforded in each situation regardless of the method.

The critical factor will be to integrate the local verification of the end user in the private domain in relation to his/her token, performed with biometrics, with the cryptographic solutions for identification supported by these tokens.

As active members of GP and FIDO we are attempting to advance the understanding, practical usability and availability of biometrics as a means for verification in open standard authentication environments. We believe the following questions need addressing in order for biometrics to fully provide the support for multifactor authentication that it clearly has the potential of doing.

Privacy Issues

Are there any privacy implications of biometrics in token multifactor authentication schemes? Are there any real concerns and how can they be mitigated? What are the critical requirements and design issues for achieving privacy protection in a token based multifactor authentication environment, how are they affected when biometrics are used?
In spite of the fact that biometric information is to a large part available in the public domain, through e.g. pictures on Facebook etc., and the fact that according to EU regulation biometrics are not considered sensitive personal information, still experience shows that to the end user community the handling and containment of biometric information is regarded as highly important and personal. We consider that the possibility of providing credibly and verifiably protected private storage of biometric information will become part of any successful service and of the User Experience.

Proposal

We propose that there are no more privacy issues in using a token which performs local verification against locally stored templates of biometrics than with any recognized user verification method. This provided that the biometric information is strictly stored and processed only in the token owned and controlled by the end user.

We would like to explore if and how the security of the local storage of biometric information could be enhanced by support from the server side in communicating tokens which are capable of exchanges with the Relying Party or the Certificate Authority or other services.