P2410

Submitter Email: xillia@ieee.org
Type of Project: Revision to IEEE Standard 2410-2015
PAR Request Date: 29-Apr-2016
PAR Approval Date: 30-Jun-2016
PAR Expiration Date: 31-Dec-2020
Status: PAR for a Revision to an existing IEEE Standard
Root Project: 2410-2015

1.1 Project Number: P2410
1.2 Type of Document: Standard
1.3 Life Cycle: Full Use

2.1 Title: Standard for Biometric Open Protocol **Changes in title:** ~~IEEE~~ Standard for Biometric Open Protocol

3.1 Working Group: Biometrics Open Protocol (COM/SDB/BOP)
Contact Information for Working Group Chair
Name: Scott Streit
Email Address: scott@scottstreit.com
Phone: 301-596-2550
Contact Information for Working Group Vice-Chair
Name: Clayton Stewart
Email Address: cstewart14@sky.com
Phone: +447889124115

3.2 Sponsoring Society and Committee: IEEE Communications Society/Standards Development Board (COM/SDB)
Contact Information for Sponsor Chair
Name: Mehmet Ulema
Email Address: m.ulema@ieee.org
Phone: +1 732 957-0924
Contact Information for Standards Representative
Name: Mehmet Ulema
Email Address: m.ulema@ieee.org
Phone: +1 732 957-0924

3.3 Joint Sponsor: IEEE Council on RFID/Standards Committee (CRFID/SC)
Contact Information for Sponsor Chair
Name: William Lumpkins
Email Address: xillia@ieee.org
Phone: 972-639-6393
Contact Information for Standards Representative
None

4.1 Type of Ballot: Individual
4.2 Expected Date of submission of draft to the IEEE-SA for Initial Sponsor Ballot: 11/2016
4.3 Projected Completion Date for Submittal to RevCom
Note: Usual minimum time between initial sponsor ballot and submission to Revcom is 6 months.: 10/2017

5.1 Approximate number of people expected to be actively involved in the development of this project: 41
5.2 Scope: The Biometric Open Protocol Standard (BOPS) provides identity assertion, role gathering, multilevel access control, assurance, and auditing. The BOPS implementation includes software running on a client device (e.g., smartphone or mobile device), a trusted BOPS Server, and an intrusion detection system (IDS). The BOPS implementation allows pluggable components to replace existing components' functionality, accepting integration into the current operating environments in a short period of time. The BOPS implementation adheres to the principle of continuous protection in adjudicating access to resources. Accountability is the mechanism that proves a service-level guarantee of security. The BOPS implementation allows the systems to meet security needs by using the application programming interface (API). The BOPS implementation need not know whether the underlying system is a relational database management system (RDBMS) or a search engine. The BOPS implementation functionality offers a "point-and-cut" mechanism to add the appropriate security to the production systems

as well as to the systems in development.

5.3 Is the completion of this standard dependent upon the completion of another standard: No
5.4 Purpose: This standard provides a biometric-agnostic, multilevel security protocol.

5.5 Need for the Project: Convenience drives consumers toward the biometrics based access management solutions; say studies from Ericsson, PayPal, IBM, and Microsoft.
According to the Ericsson's study "Your body is the new password", 52 percent of smartphone users want to use their fingerprints instead of the passwords, a further 61 percent want to use fingerprints to unlock their phones, and 48 percent want to use eye-recognition.
The study conducted by PayPal says that consumers approve biometrics for access management. In terms of readiness to switch from an old fashion password protection to the new technology, 53 percent of surveyed population would be comfortable replacing passwords with the fingerprints and 45 percent would choose a retinal scan, which is presumably an iris scan - the misplaced terminology points to the lack of a consumer education.IBM Fellow and Speech CTO David Nahamoo states that over the next five years, your unique biological identity and biometric data - facial
definitions, iris scans, voice files, even your DNA - will become the key to the safeguarding of your personal identity and information and will replace the current user ID and password system.
Microsoft Research funded a study that titled "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes", the cornerstone conclusion of which indicates that the vast passwords replacement transition should conform to the following criteria: nothing to carry, efficient to use, and easy recovery from a loss. The Microsoft study goes as far as concluding such criteria could be achieved mostly in the biometric schemes.
Biometric technologies provide consumer with a long-awaited convenience to securely enter into the cyberspace on the frontend. The Biometric Open Standards protects digital assets and digital identities on the back-end.

5.6 Stakeholders for the Standard: Consumer electronic and mobile product developers, banking, including ATMs, Point of Sale, Automotive. Basically any system needing identity or end to end security.

Intellectual Property
6.1.a. Is the Sponsor aware of any copyright permissions needed for this project?: No
6.1.b. Is the Sponsor aware of possible registration activity related to this project?: No

---

7.1 Are there other standards or projects with a similar scope?: No
7.2 Joint Development
Is it the intent to develop this document jointly with another organization?: No

---

8.1 Additional Explanatory Notes: