Comments Resolution on OASIS Biometric Open Protocol Specification (BOPS) Technical Committee (TC) draft charter

https://lists.oasis-open.org/archives/oasis-charter-discuss/201407/msg00000.html

Date: 07/23/2014	Document: **Comment Resolution BOPS TC**	Convenor Name Abbie Barbir

Comment Source	Comment type	Comments	Proposed change	Resolution
Robin Cover <robin@oasis-open.org>		https://lists.oasis-open.org/archives/oasis-charter-discuss/201407/msg00004.html		
	ED	TC name in Proposed Charter for OASIS Biometric Open Protocol (BOPS) TC Minor comment on the BOPS TC name as proposed -- actually, a comment from earlier OASIS Staff conversations that got lost in the weeds or fell through the cracks... The current proposal [1] suggests (1)(a) a TC name: OASIS Biometric Open Protocol (BOPS) TC Our observation is that the acronym BOPS contains "S", but the remaining portion of the TC name provides no clue as to what "S" stands for in the acronym expansion. People will wonder what "S" means, and they will (variably) then invent some candidate, and promulgate variant name elements for "S". The referent of "S" needs to be clear in the TC name itself.	I think it would be acceptable to change the name to: OASIS Biometric Open Protocol Specification (BOPS) TC That name asserts that the TC is working on a "specification" which is an open "protocol" for biometrics. Another theoretical possibility for "S" would be "Standard", but I don't think the term "Standard" is appropriate in a TC name. That has proven problematic in a couple cases where we have experience. Ideally, in any SSO/SDO "Working Group" or "Technical Committee" or "Working Party", the goal may be to develop, advance, and approve a specification to the highest level of maturity. But in OASIS, as elsewhere, "Standard" in a label/attribute assigned to a specification -- Not a qualifier for a TC (embedded in a TC name)	Noted. TC name will be changed.
Chet Ensign		https://lists.oasis-open.org/archives/oasis-charter-discuss/201407/msg00005.html		
		Alternatively you could just drop the "S" and leave it as BOP.	Alternatively you could just drop the "S" and leave it as BOP.	noted

Comments Resolution on OASIS Biometric Open Protocol Specification (BOPS) Technical Committee (TC) draft charter

https://lists.oasis-open.org/archives/oasis-charter-discuss/201407/msg00000.html

Date: 07/23/2014	Document: **Comment Resolution BOPS TC**	Convenor Name Abbie Barbir

Accenture				
	TE	"One of our highest priorities in the information security field is the development of techniques to confirm that a person accessing online resources is authorized and allowed to do so. Simply stated, an entity must be able to validate its identity before accessing information, otherwise access to a resource should be denied. "	Authentication and Authorization are two distinct functions which are not interchangeable as implied here. Suggest that the wording be changed accordingly.	Noted. Fixed language
	TE	"Much of the recent enterprise-level security breaches have been made by hackers with targeted activities to steal clients' information for fraud and identity theft. This trend has enhanced awareness for the need for better authentication methods to prevent crime and fraud at all levels."	This is speculative and, without specific reference(s), should be deleted.	Noted. Fixed language.
	TE	"Until recently, the "something that we are" authentication method, such as biometrics technology, was resource intensive. However, the advent of smart phones, smart watches and mobile devices that include sensors (such as cameras, fingerprint scanners and microphones) has made it feasible and affordable to use biometrics for identification and authentication for online access. Biometrics systems can identify users based on either physiological or behavioral characteristics."	However, the advent of smart phones, smart watches and mobile devices that include sensors (such as cameras, fingerprint scanners**, ~~and~~** microphones, **and GPS**) has made it feasible and affordable to use biometrics for **~~identification and~~** authentication for online access. **~~Biometrics~~ Recognition** systems can identify users based on either physiological or behavioral characteristics **along with contextual information**.	Noted. Fixed language
	TE	"The demand for the ease and reliability offered by biometrics is growing. Consumers want security systems in place that prevent unauthorized access to their personal data. They are also concerned about having their identities stolen and used by thieves. Individuals have password fatigue and tend to reuse passwords across many sites, which add to the risk of identity theft and fraud. At present, biometrics technology holds a great deal of promise as the solution the industry has been searching for--but it is not without its limitations and certainly not without its critics."	Again, confusing Authentication and Authorization; biometrics can aid in the former but not the latter: "The demand for the ease and reliability offered by biometrics is growing. **~~Consumers want security systems in place that prevent unauthorized access~~**	Noted. Fixed language

			~~to their personal data. They are also concerned about having their identities stolen and used by thieves~~. Individuals have password fatigue and tend to reuse passwords across many sites, which add to the risk of identity theft and fraud. At present, biometrics technology holds a great deal of promise as the solution the industry has been searching for--but it is not without its limitations and certainly not without its critics.	
"Raul Sanchez-Reillo" <rsreillo@ing.uc3m.es>	Te	I do not have a clear idea of what the new TC is proposing as a protocol. Is it a communication protocol? An authentication protocol? A cryptographic protocol? etc. It is also important to see why this work has to be covered by a new TC, instead of using either the OASIS TC on Biometrics, or even the ISO/IEC JTC1/SC37. If this work is intended to create a biometric authentication protocol in client-server application, then the work of the experts proposing the creation of the new TC, may benefit from joining any of both above mentioned standardization bodies. In fact, that work could be a layer over BIAS (formerly defined by OASIS and currently adopted by ISO/IEC JTC1/SC37 in the 30108 standard). The creation of a new standardization body will disagregate the	No suggestions provided for improving text	Noted. Text is improved to address the questions. BOPS do not overlap with other ISO standards and it is not designed to compete with them.

		standardization effort, and that will be really bad for the industry. Therefore I'd like to discourage the proposers about the creation of such new TC, and invite them to join either OASIS Biometrics TC or ISO/IEC JTC1/SC37.		
Microsoft		https://lists.oasis-open.org/archives/oasis-charter-discuss/201407/msg00001.html		
		Please find the enclosed comment on the proposed charter: Statement of Purpose: 1. This charter is very hard to understand relative to the "the purpose", it is very unclear if this charter is about identification or about authentication or even authorization, maybe you are trying to do all these things? Suggest you clarify the exact purpose of this TC. Reading through the whole charter it seems the proposal is to create something that provides Identity assertions, role gathering, multilevel access control and auditing. Also it will provide continuous protection of resources and assure placement and viability of adjudication and other key features. Later in the deliverable section you also talk about "criteria necessary for intrusion detection". So I'm very confused as what this TC is really proposing to do. 2. The charter states that there "are some" use cases that require the enterprise or the provider to store the biometric information on the local server, but never gives any examples of these use cases. For the most part the industry has chosen not to have biometric data leave the local device due to privacy concerns, this charter does not address the privacy concerns or even mentions any privacy issues.	No proposed text	Noted. Charter improved to address points 1. Point 2 is addressed by adding use case and gap analysis deliverable. 3. Solution can be used by enterprises and consumers 4. Both API and protocol will be developed. 5. Authorization is not the focus of the work. 6. Deleted registered developers. The intend was for developers in a company or an organizations 7. Noted 8. Fixed the text 9. Fixed Don Thibeau issues.

		3. It is unclear if this effort is geared towards consumers, developers or enterprises as the wording changes throughout the charter 4. It is very unclear if this is charter is about developing APIs or a protocol maybe both? The TC name indicates a protocol but charter talks about API 5. The charter says that the aim is "to protect digital assets and digital identities on the server" so it's not clear what this means is this an authorization mechanism ? 6. "BOPS will define a biometrics-agnostic standard API for registered developers" not sure what a registered developer is ? Suggest you clarify. 7. "BOPS will not compete with other standards like FIDO" not sure what this means since this is an actual alternative to FIDO, I understand it is going after a different undefined use case but the charter indicates that it will be creating a new API and protocol, thus it seems it will be competing with other standards, suggest that this sentence be removed 8. "BOPS may be used as the sole security mechanism", and in the paragraph prior to this you state that TLS/SSL or secure transport is needed and that the BOPS server must be protected against threats and attacks, so it unclear what you mean by sole security mechanism. TC Proposers 1. Don Thibeaux, I assume you mean Don Thibeau. Also Don does not have the ability to represent Open Identity Exchange, so Don would have to represent himself and I'm not sure of his OASIS status as a individual member.		
Tony Nadalin	TE	As a follow on comment, I would like to understand the rational for the selection of IPR that was chosen for the operation of the TC and why a license would be required as this seems a little odd to select RF on Limited Terms	No proposed text	Changing IPR mode to non-assert mode

Comments Resolution on OASIS Biometric Open Protocol Specification (BOPS) Technical Committee (TC) draft charter

https://lists.oasis-open.org/archives/oasis-charter-discuss/201407/msg00000.html

Date: 07/23/2014	Document: **Comment Resolution BOPS TC**	Convenor Name Abbie Barbir

Oracle		https://lists.oasis-open.org/archives/oasis-charter-discuss/201407/msg00019.html		
Hal Lockhart <hal.lockhart@oracle.com>		I noticed that amongst the proposers of this TC the only organization that seemed to be focused on biometrics is HOYOS Labs Corp. After a little public research, I learned that on Jan 7, 2014 HOYOS Labs announced a document called Biometric Open Protocol Standard (BOPS). http://www.hoyoslabs.com/newsroom/press-release/hoyos-labs-issues-biometric-open-protocol-standard-for-safer-authentication http://www.prnewswire.com/news-releases/hoyos-labs-issues-biometric-open-protocol-standard-for-safer-authentication-239034831.html The description of BOPS in the press release sounds very similar to the text of the proposed BOPS TC Charter. The cited article above states "The entire BOPS document is available upon request from Hoyos Labs at no cost, with a properly executed non-disclosure agreement between the party who is requesting it and Hoyos Labs. Please contact: hoyos@kcsa.com." I sent an email to the above address on July 15, 2014 but have received no reply yet. (KCSA is apparently a marketing communications company.) I also noted that Scott Streit, who is one of the proposers, lists his affiliation (quite correctly) as Villanova University, however he is also listed on the HOYOS Lab web site as Chief Scientist of HOYOS Labs. Also on the web site I observed a press release from Feb 13, 2014 announcing that HOYOS Labs has given Villanova University a research grant of $78,000.	Comments inside the text	Noted. Thanks for the request. Hoyos Labs will provide all needed statements. Scott will clarify all of his roles and responsibilities. Will fix the spelling.

Comments Resolution on OASIS Biometric Open Protocol Specification (BOPS) Technical Committee (TC) draft charter

https://lists.oasis-open.org/archives/oasis-charter-discuss/201407/msg00000.html

Date: 07/23/2014	Document: **Comment Resolution BOPS TC**	Convenor Name Abbie Barbir

		The OASIS IPR Policy states: "Neither Contributions nor Feedback that are subject to any requirement of confidentiality may be considered in any part of the OASIS Technical Committee Process. All Contributions and Feedback will therefore be deemed to have been submitted on a non-confidential basis, notwithstanding any markings or representations to the contrary, and OASIS shall have no obligation to treat any such material as confidential." Elsewhere it states: "Trademarks or service marks that are not owned by OASIS shall not be used by OASIS, except as approved by the OASIS Board of Directors, to refer to work conducted at OASIS, including the use in the name of an OASIS TC, an OASIS Deliverable, or incorporated into such work." I am not accusing anyone of acting in bad faith here. I am sure that unfamiliarity with OASIS policies is the explanation. At a minimum I would like the following. A statement from HOYOS Labs stating that it has no IPR claim of any kind on the name "Biometric Open Protocol Standard" or "BOPS". A statement from HOYOS Labs about whether they intend to contribute their "BOPS" document to the TC and if so, that they understand the requirements of the OASIS IPR Policy. Finally, while it is not required by the TC Process, I would suggest in the interests of openness that Scott Streit's membership of the HOYOS Lab senior management be disclosed in the charter or somewhere else that will be easily visible to OASIS members. P.S. Hector Hoyos's name is misspelled in the Proposer's section, although his email address and company name (both containing Hoyos) are correct.		

Comments Resolution on OASIS Biometric Open Protocol Specification (BOPS) Technical Committee (TC) draft charter

https://lists.oasis-open.org/archives/oasis-charter-discuss/201407/msg00000.html

Date: 07/23/2014	Document: **Comment Resolution BOPS TC**	Convenor Name Abbie Barbir

NIST		**https://lists.oasis-open.org/archives/oasis-charter-discuss/201407/msg00006.html**		
"Brady, Mary" <mary.brady@nist.gov>		To OASIS and interested parties in biometric technology and standardization: We appreciate the opportunity to provide feedback on the draft charter of the proposed BOPS TC. NIST is heavily involved in the work of the OASIS Biometrics TC and the ISO/IEC JTC1 Subcommittee 37 on Biometrics, working alongside the biometric companies, consumers, researchers, and testing labs in this space. As a member of both organizations, we would like to provide our own observations and questions regarding the proposed new TC. 1. We would like to draw your attention to the comments and the work of both ISO/IEC JTC 1 SC 37 and the OASIS Biometrics TC to help inform the needs of the proposers of the new BOPS TC. These are two key fora where biometric experts convene and develop standards that are being adopted globally. 2. The description of the new TC is broad. As proposed, this new TC would collide with existing work in ISO/IEC JTC 1 SC 37 and potentially the OASIS Biometrics TC and ISO/IEC JTC 1 Subcommittee 27 (IT security techniques). The information provided does not identify a standards gap that is going to be filled by starting a new committee. 3. We believe that technical standards have the best chance for success when developed by experts and other stakeholders. Whenever possible, we advise starting new standards projects in committees where the experts are already convening and that have a track record for developing standards that are being used in the marketplace. 4. OASIS has a proven track record for producing successful	No proposed text for updating the charter was included.	All comments are noted. 1,2,3,4,5. Relationship to OASIS BIAS and biometric and ISO work was included in the charter. The scope is better explained and input from NIST was adopted. OASIS process allow a TC to decide how it will further standardize its work and ITU and ISO are within OASIS accepted process.

		international standards. ◦ In addition, OASIS is an ISO/IEC JTC 1 PAS submitter, which provides a fast track pathway to produce ISO standards from OASIS, that can be used to remove barriers to trade if that is needed for global acceptance (depending upon the policies or laws of other countries or regions that may use products or services conforming to the standard). ◦ We do not know of a compelling reason to start joint projects with another standards organization for the proposed work (as opposed to utilizing liaison statements or other similar tools), which introduces complexity and can increase the time to produce a standard. If there is reason, the other standards body should have a track record for producing successful standards in the technical area of interest (in this case, biometric authentication) and participants who are experts in the technical area of the standards project(s). ◦ Similarly, there should be a compelling reason for OASIS to ask another standards body to adopt their work. If there is reason, the other standards body should have a track record for producing successful standards in the technical area of interest (in this case, biometric authentication) and participants who are experts in the technical area of the standards project(s). In summary, a better description and scope of the proposed project and its relationship to relevant biometrics standards (published and under development) is needed. Then, placement of any new work should consider the two existing major fora for biometrics standards work (OASIS Biometrics TC and JTC 1 SC 37) or possibly JTC 1 SC 27 if the project work is intended to focus on security. Please let us know if you would like to discuss our comments further.		

Comments Resolution on OASIS Biometric Open Protocol Specification (BOPS) Technical Committee (TC) draft charter

https://lists.oasis-open.org/archives/oasis-charter-discuss/201407/msg00000.html

Date: 07/23/2014	Document: **Comment Resolution BOPS TC**	Convenor Name Abbie Barbir

OASIS Biometric TC		**https://lists.oasis-open.org/archives/oasis-charter-discuss/201407/msg00013.html**		
"Mangold, Kevin C." <kevin.mangold@nist.gov>		General 1. If this project heavily involves web services, consider putting this project in the OASIS Biometrics TC, which already has both biometrics and web service experts involved, as well as liaison relationships with other relevant/similar committees in other SDOs. You can view the charter at https://www.oasis-open.org/committees/biometrics/charter.php 2. Section 1b a. Statement of Purpose is unclear; what is BOPS and what will it solve? b. NIST 800-52 Revision 1, Section 3.1, paragraphs 1-2 advise to use TLS 1.1+; remove SSL from SOP and clarify that TLS 1.0 shall not be used. c. "biometrics-agnostic standard API for registered developers" – What does it mean to be a "registered developer"? How would one register? Are there any fees involved? Will the chosen IPR mode conflict with this registration process? 3. Section 1c a. Scope is unclear; what is BOPS and what will it solve? 4. Section 2a a. Is there really NO other being done by another organization or SDO that has any similarities to BOPS? How is the IEEE P2410 BOPS project (http://standards.ieee.org/develop/project/2410.html, http://standards.ieee.org/develop/wg/BOP.html) related? For example, biometric image quality might use ISO standards, interfaces to matchers & sensors might use specifications developed	Proposed text within comments received	Comments Noted. • NOTE: This feedback is supposed to be from OASIS Biometric TC. Can you please point to the approved TC meeting minutes (including date, time and people in attendance) that enabled the TC to send the feedback? 1. For point 1, this is not a project. It is a proposal for new TC. Scope of the BOPS is not the same as the biometric TC. 2. Comments on Section 1b). TLS is used now. Scope is improved and the use of registered developers has been deleted. 3. Comments on Section 1c, noted, scope has been improved 4. Comments on Section 2a, BOPS in OASIS will coordinate with all needed OASIS TC. No joint projects with any SDO but coordination through Liaison activities and may be further standardization through PAS in ISO or Submissions to ITU. 5. Comment on Section 2b. Noted will add details of telecom. 6. The TC will coordinate and work closely with the IEEE Project P2410 (BOP).

		by the OASIS Biometrics TC. b. Please explicitly state which committees within each SDO you plan to coordinate with. Will this be a liaison relationship or joint work? c. Current committees with Biometrics expertise are the OASIS Biometrics TC, INCITS M1, ISO/IEC JTC 1 SC 37. ISO/IEC JTC 1 SC 27 may be in scope as it contains IT Security and Identity Management experts. 5. Section 2b a. The first I TC meeting must have dial-in information (TC Process 2.3, paragraph 1; TC Process 2.10, paragraph 1)		
DOAN		**https://lists.oasis-open.org/archives/oasis-charter-discuss/201407/msg00014.html**		
"Tilton, Cathy" <Cathy.Tilton@daon.com>		Please find Daon's comments on the proposed Biometric Open Protocol Standard (BOPS) TC below. We are pleased to see an on-going interest within OASIS regarding the area of biometric technology and its standardization. We also appreciate the opportunity to provide feedback on the draft charter of the proposed BOPS TC. --- COMMENTS 1. We are pleased to see continuing interest within OASIS in the area of biometrics. We are wondering, however, if this project might be better placed within the existing OASIS Biometrics TC? 2. The first 7 paragraphs of the Statement of Purpose provide background information to aid in understanding the problem and are therefore useful for this purpose. After that, the discussion becomes a bit confusing. 3. It is unclear exactly what is proposed to be standardized. Is it: a. A biometric <web> server API?* b. An authentication protocol? c. A security mechanism?	See Comments	Noted 1. NO BOPS Charter does not fit in OASIS Biometric TC 2. Noted 3. Noted. Scope improved. 4. It can include any client. 5. New scope improve the text 6. Text fixed 7. Noted 8. Noted 9. Noted. TC can decide on relevant liaison activities once it is in operations

		*Please note the existence of the Biometric Identity Assurance Services (BIAS) standard (INCITS 442, OASIS BIAS SOAP Profile, ISO/IEC 30108) which could be leveraged for this purpose. 4. (1)(b) paragraph 5 mentions mobile devices and (1)(c) mentions Android/iPhone as client devices. Does the target architecture include any client or just mobile clients? (Note: A conceptual architecture diagram would be helpful.) 5. It is not clear what the target component(s) is with respect to protection/security. Is it biometric data in transit or at rest or both? Intrusion detection is also mentioned, but it is not clear how this relates. Is auditing a BOPS capability or is this merely meant to be supported by the BOPS interface? 6. In the Scope section, the charter indicates that BOPS is to be language/implementation neutral, but then says it is to be built upon OpenSSL, Java, JSON, REST, and Apache Solr. Does this mean that BOPS will be specified independent of language but that bindings will be provided for each of these? 7. Under Deliverables, the first subparagraph of paragraph 1 appears to equate liveness detection and intrusion detection which is misleading. Further, it implies that BOPS will be server based, but then discusses security features of biometric devices (sensors) associated with anti-spoofing mechanisms. Is this intended to mean that the BOPS API will support transmission of liveness information? (Note: You may wish to consult/reference ISO/IEC 30106, Presentation Attack Detection, in progress, for more information if BOPS is indeed intended to address this area.) 8. (1)(f) Audience “guarantees” risk mitigation. It is recommended to use less provocative language. 9. (2)(a) mentions ISO as a potential liaison/source of		

		similar work. Please see a list of potentially relevant project within ISO/IEC JTC1 SC37 below. In addition to OASIS, Daon participates in the work of ISO/IEC JTC1 SC37 subcommitee on biometrics. As such, we would like to draw your attention to some of the work of SC37 that could both help inform the work of the new BOPS TC as well as potentially be leveraged within the resulting BOPS protocol (i.e., as either an informative or normative reference). In particular, within the SC37 portfolio of biometric standards and technical reports are the following: · ISO/IEC DIS 30108, Biometric Identity Assurance Services (BIAS). This standard, nearing publication, is an international version extending the work of INCITS 442 (also the basis for the existing OASIS BIAS SOAP profile). This standard defines a set of operations for invoking biometric services over a service oriented framework. · ISO/IEC TR 30125 Biometrics used with mobile devices. . This technical report provides guidance for developing a consistent and secure method of biometric (either alone or supported by non-biometric) personalization and authentication in a mobile environment. · ISO/IEC 19794, Biometric data interchange formats. This multi-part standard specifies the format of biometric data records for various biometric modalities, including binary and (in progress) XML formats, to support interoperability among biometric systems and components. Formats to date include fingerprint (image, minutiae, pattern/spectral & skeletal), face, iris, signature/sign (time series and processed dynamic data), vascular, hand geometry, DNA and fusion information. · ISO/IEC 19785, Common Biometric Exchange		

		Formats Framework. This standard defines a metadata structure for exchanging biometric data. The OASIS BIAS SOAP Profile specifies a CBEFF XML format instantiation. · ISO/IEC 29794, Biometric sample quality. This standard defines the format for the exchange of quality metrics. Modality specific metrics are defined as individual parts. · ISO/IEC 19795, Biometric performance testing and reporting. This standard defines the methodology and measurements associated with biometric performance evaluation (e.g., accuracy). · ISO/IEC TR 24722, Technical report on multi-modal and other multi-biometric fusion. This report provides a description of and analysis of current practice on multimodal and other multibiometric fusion. · ISO/IEC WD 30107, Presentation attack detection. This in-progress three-part standard addresses terminology, data format, and performance testing and reporting associated with liveness/spoofing and other attacks when a fake biometric is presented at the sensor. We believe that to be effective, the development of any biometric authentication protocol should consider such things as interoperability, performance, security, and industry best practices. We hope that by providing the above references, the BOPS TC will be better informed about resources available to enhance the capability of its specification.		
Noblis		**https://lists.oasis-open.org/archives/oasis-charter-discuss/201407/msg00015.html**		
	GE	The OASIS Biometric Open Protocol Specification (BOPS)	State more clearly how this work is	Noted. Text Improved

Comments Resolution on OASIS Biometric Open Protocol Specification (BOPS) Technical Committee (TC) draft charter

https://lists.oasis-open.org/archives/oasis-charter-discuss/201407/msg00000.html

Date: 07/23/2014	Document: **Comment Resolution BOPS TC**	Convenor Name Abbie Barbir

		Technical Committee (TC) draft charter makes mention of expertise and existing work in biometrics (INCITS M1 – Biometrics, JTC 1/SC 37 – Biometrics), web services (OASIS Biometrics TC), and IT Security Techniques (INCITS CS1, JTC 1/SC 27). More specific comments follow.	separate, distinct, non-duplicative of, and will liaise with the work of other entities involved in biometrics, web services, and IT Security Techniques.	
	TE	The OASIS BOPS TC draft charter makes no mention of the existing OASIS Biometrics TC. Why is this TC being proposed independent of, with no acknowledgement of, nor liaison with the existing OASIS Biometrics TC?	Propose this effort as a deliverable of the existing OASIS Biometrics TC – or – State clearly in a revised BOPS TC draft charter why this effort is separate, distinct, non-duplicative of, and will liaise with the work of the existing OASIS Biometrics TC.	Noted. BOPS charter improved
	TE	The OASIS BOPS TC draft charter makes no mention of expertise and existing work in biometrics (INCITS M1 – Biometrics, JTC 1/SC37 – Biometrics). Whether this effort progresses as a separate TC or as a deliverable of the OASIS Biometrics TC, it should reference existing and developing standards of SC 37 – Biometrics.	Reference existing and developing standards of SC 37 – Biometrics, e.g. - 19794, Information technology -- Biometric data interchange formats - 29794, Information technology -- Biometric sample quality - 30108, Biometric Identity Assurance Services (BIAS) - 30125, Biometrics used with mobile devices	Noted. Relevant work was added.
	TE	The Statement of Purpose and Scope are not in agreement. The Statement of Purpose states, “This goal of this Technical Committee is to develop the Biometric Open Protocol Standard (BOPS) with the aim to protect digital assets and digital identities on the server”. The Scope states “BOPS will define how software running on a client device…”.	Revise the Statement of Purpose and Scope to state clearly whether this effort will protect digital assets on the server, the client, or both.	Noted. Text improved
	TE	The OASIS BOPS TC draft charter states “The solution offers the minimum criteria necessary for liveness…”, but makes no mention of the work in this area in JTC 1 / SC 37; specifically the multi-part standard ISO/IEC 30107, Presentation Attack Detection (PAD). Whether this effort progresses as a separate TC or as a deliverable of the OASIS Biometrics TC, it should reference the work of ISO/IEC 30107.	Insert reference(s) to ISO/IEC 30107, Presentation Attack Detection.	Noted.
	TE	(2)(a) States incorrectly there is no similar work underway.	State clearly how this effort relates to:	Noted. Disagree. Text improved.

			• INCITS B10 – Identification Cards and Related Devices • INCITS CS1 – Cybersecurity • INCITS M1 – Biometrics • JTC 1/SC 17 – Cards and personal identification • JTC 1/SC 27 – IT Security Techniques • JTC 1/SC 37 – Biometrics OASIS Biometrics TC	
Additional comments that were sent to OASIS. This came from OASIS Staff.				
1		1 b) Minor typo (wrong name) : The Fast Identity Alliance (FIDO) Should be: The Fast Identity Online (FIDO) Alliance Minor typo (too wordy): "There are some use cases that require that the enterprise or the provider to store the biometric information on local servers in order to provide enhanced biometric solutions" Should be there are some use cases that require the enterprise or provider to store biometric information on local servers in order to provide enhanced biometric solutions Question: "point and cut" Is "point and cut" a good analogy? It does not clearly describe the intended behavior.	See submitted text	Noted. Fixes included. Text improved.

		1d) Question? "This solution will consider pluggable initial setup for a user called genesis or enrollment." Why do I care about the user names? Is there any significance? If not, should be removed. Overall: The article suggests that Biometrics alone can validate someone's identity without risk. There should be some discussion of the risk of "false negatives" and "false positives".		
2		1. "Federation technologies, coupled with national and industry-specific trust frameworks, are emerging as a viable solution to weaker methods of authentication based on user name and password. " Federated identity does not necessarily mean replacement of user name and password. The means of authentication in a federated environment is usually not specified, or is an option depending on trust level or a community's requirements. One can have federation and still have passwords, and one can get rid of passwords without federation. So, I don't see how federation technologies are a "solution to weaker methods of authentication". That said, in that federation delegates authentication to specialists (maybe), stronger authentication may be more likely. However, in practice, federation with Facebook or Google as the authenticators has not made authentication any stronger. 2. "... to servers that employ Intrusion Detection Systems (IDS)" Why emphasize IDS? There are other security functions (IPS, WAF, others). I wonder why IDS is singled out? 3. "BOPS will define a biometrics-agnostic standard API ..."	See text	Noted. The idea was that stronger authentication could benefit parties within a federation. Test fixed on IDS. Improved text on API and Protocol Took out Java/JASON etc.

		The 'P' in BOPS is Protocol, but BOPS will define an API. Maybe it's obvious, but I presume BOPS will define both a protocol and an API? 4. "The BOPS architecture will be language-neutral, ... The architecture will be built on the servlet specification, open secure socket layers, Java, JSON, REST, and Apache Solr." Odd to see "language-neutral" and "Java" in the same sentence. If BOPS architecture is built on Java, how is it language neutral? Where does Solr fit into this? 5. I am sympathetic with choice of JSON, but that immediately raises the question of how to secure it in a standard way. Both JWS and JWE are still drafts, although there are implementations. But maybe that's a discussion for later in the process. 6. "... address use cases that require the relying party to have access to biometric information." Is "relying party" really intended here? Yes, a server has access to the biometric information, but in a federated identity system why would the relying party require this accsss? The identity provider would do so. If the relying party and identity provider is the same entity, so be it. But shouldn't the charter support uses cases of "pure" federation? 7. It is very surprising to me to see a charter regarding server based biometric that does not even include the word "privacy" once.		
3		I think the organization of the effort and the committees and sub groups is excellent. One area which is missing is someone to do the "marketing and education" to the	See text	Noted and agree. We will try to educate as much as we can.

		audience to which you are directing the work. There are a number of Bio-metric efforts being started such as "FIDO" and relative to government actions, the "Bio-Metric" Consortium was founded by NIST, DoD, and the NSA and see textsince I live in all those worlds, I am aware that some in DoD and NIST, for example, are going down the same path, but their leadership don't know one another and have no plans for collaboration. Some participants are working in all the groups, such as Financial Institutions. It would be good if the Oasis group could reach out and collaborate with the "Bio-Metric Consortium", which is run by our government and my guess is that government agencies concerned with healthcare will want to use what is developed for legal and ease of use reasons. To do this well would require a formalized approach which OASIS could do? If Oasis doesn't collaborate with the Bio-metric Consortium, this will cause confusion in the stakeholders and they won't know "what" to do? HIMSS has a Security & Privacy effort led by a "Lisa Gallagher" and within the State of Michigan; [...] the "Federated Hub" effort shall include the use of a Bio-Metric, relative to Section 5 of NIST 800-63 for "two-factor" authentication. Authentication is important in the state of Michigan, as we have written a machine readable "consent management" document, which has passed our Legislature and is signed by our Governor and authentication is an important part of the process to be determined and [,,,] there shall be many different vendors selected by various stakeholders and organizations. When you look at "FIDO", you'll find a number of financial institutions and as FI's , we have begun an effort to example how we can roll out bio-metric solutions as an industry, in for example, the mobile space. Many questions here. Education of the models developed should be considered by the Oasis effort and as I've noted in other venues, "we all need to come out of our silos and start talking to one another" as I believe a solution will not be deployed without		

		a period of testing and validation as people will have fear and will/have drag their feet on deployment as the corporate people who control the budgets, have to align the bio-metric solutions and what they bring to the table, to automate the process of bio-metrics for access control and audit. One basic question is: If the biometric is "bound" to a certificate (x509) with the policies and attributes in "code", how do you "know" in "real time" that the "policies" you "think" are bound in the cert, are actually functioning in the manner in which you expect? My final comment, which may be outside the scope considered is "who" or "what" is going to train organization personnel on the work OASIS generates? As vendors might say to customers, "you don't need that"! (smile)		
4		do you engage with the UK Government Digital Services Standards team at all in relation to identity assurance related standards (Matt Trigg, Justin White, Howard Staple)?	See text	Noted. Will add that to the first deliverable
5		Here our comments related to BOPS: BOPS claims to create a uniform standard for proper use and secure application of biometrics in an Identity Assertion environment with goal Authentication: what is exactly what SAML does without concentrating on biometrics. We do not understand at this point why a new standard makes more sense than extended an existing and accepted one to cover the missing details. BOBS authenticates between a user and particular service: this is again the role of an Identity Provider defined already in the SAML standard	Suggestion are in the text	Noted. Disagree BOPS solve different set of problems and it can definitely help extend the reach of SAML

		BOPS does not require a token: From our viewpoint it should not be standardized at all if a token is needed or not in an universal authentication standard with or without biometrics. Our philosophy follows the fact that the requesting application rarely needs a specific authentication method but needs context specific a specific strength of authentication. The method can vary dependent on the scenario (environment, form factor of device, location...) BOPS defines that the biometric data and the matching shall always be on the mobile device but that the private key generation is only in the secured backend: if the biometrics are kept on the mobile device this device must be very secure as the biometric data are very valuable data. A mobile device capable having biometric data and match on it should have a secure storage and a own processing unit completely separated from the rest of the device (see e.g. iphone architecture, and in a more general way payment terminals although not dealing with biometrics). Such a device should be secure enough to store a private key (certificate). Furthermore when the biometric authentication is done on the mobile but the private key that identifies the user+application combination later to the service is generated on the server back-end the authenticator and identity provider are not the same entity. A strong trust relationship and very secure network connection is needed to implement such an architecture. This can explain why BOPS requires an Intrusion Detection System. In this case the reliability of the identity is fully dependent on the secure communication between the authenticating device and the key generating server. We see the "BOPS standard" too close to a concrete implementation. A new standard might not be the right approach to support the idea behind BOPS We think that to leverage the SAML standard to also cover biometrics would be the right way to support "biometric" identity assertions and make them available for a huge number of applications across all industries.		

Comments Resolution on OASIS Biometric Open Protocol Specification (BOPS) Technical Committee (TC) draft charter

https://lists.oasis-open.org/archives/oasis-charter-discuss/201407/msg00000.html

Date: 07/23/2014	Document: **Comment Resolution BOPS TC**	Convenor Name Abbie Barbir

6		Referring to the first sentence in (1)(c) Scope, "The TC will develop the BOPS standard to enable biometric security systems that provide Identity Assertion, Role Gathering, Multi-Level Access Control, Assurance, and Auditing." It's not clear if the BOPS standard is intended to include the provision of Identity Assertion, et al, or just address authentication for a system that provides those things. I assume the latter (to avoid reinventing the wheel), but the language could be clarified. Unless it's already been done, the group should also consider recovery when a BOPS-enabled server is breached. How does another BOPS server know that the biometrics information it receives about an individual is not derived from a breached server? I know the charter assumes that "BOPS assume (sic) that the server will be protected against threats and attacks," but we know breaches will occur, and if they cannot be addressed, BOPS will not have long-term viability.	See text	Noted. Recovery will be covered in the deliverables
7		In setting up a BOP Server the controls in place would need to be strict according to some governance standard, What would that be? The lifecycle of the enrolment data would need to be defined, i.e. how long it is stored for, who has access, and who can utilise the service? How is the REST interface secured? E.g. what prevents anyone accessing an enrolled persons finger prints for example? The working group must specify strict controls about the data storage and protection surely? WE imaging that external audits would lead to encrypting of data to ensure it remains safe. And hence, behind the	See text	BOPS will within an assurance framework like the one specified in X.1254 or ISO 29115. It will also work with OASIS Trust Elevation specifications. Yes audits can be performed.

		concept of BOPS would become certification similar to WebTrust.		
8		Our deployment with the Daon biometric service solution is perhaps unique in that it is deployed via the Attribute Exchange Network (AXN). In this model, an identity provider (IdP) would perform identity proofing to issue a user credential, and the IdP would use the AXN attribute verification services to verify user attribute assertions via credit bureaus, telcos and/or enterprise LDAP services. During the proofing process, the IdP can evoke the Daon service via the AXN to capture user biometrics (voice, face, fingerprint) using the IdP or user's mobile device that has a downloaded version of the Daon application. This creates a biometric reference file (model of the user's biometrics) in the Daon service that is linked to the user device as well but does not necessarily include user Pii in the Daon file. So, the IdP proofing process/application gathers the user asserted information (Pii), including the biometric data, verifies the user Pii via the AXN, and generates a credential for that user. The credential is thereafter provisioned to the Relying Party with relevant Pii (via the AXN flow) so the RP can create a user account. On subsequent user logins to the RP with that credential, the AXN enables the user login with that credential via the IdP authentication service. If the RP requests a biometric authentication during login, or at some subsequent point in the user interface (such as to invoke a financial transaction), the AXN invokes the Daon service via the user's mobile device to capture the user's biometric in the context of the user's transaction. The Daon service matches the direct-captured biometric with the set of biometrics on file to generate a claim (e.g., match or no-match). The AXN then pass the claim results to the RP for service authorization. The process I just outlined does not require the RP to install hardware or software in their IT environment since the IdP,	See provided text	Noted.

		Daon and AXN services are cloud services. It enables the IdP to bind the biometric verification process to their credential as a federated identity service - i.e., capture the biometrics once, and allow RPs active on the AXN to obtain verification claims about user biometrics in the context of a session and on a per transaction basis. IdPs get to proof once, and generate revenue from biometric claims across a broad array of RP use cases and transactions. This fundamentally changes the economics of biometric authentication services. As I said, this scenario is very specific the IdPs, APs, RPs and users that interact via the AXN. However, the premise of enabling biometric authentication as a federated identity service is valid, and I believe potentially very attractive to the marketplace.		
9		I have had a quick look at the draft charter and its good to see that the objective is for requirements and not solutions within the standard. By not mandating solutions, technology advancements and innovation are not constrained by legacy words. However, the downside is that evaluation and compliance of solutions becomes more than a tick-box exercise because the 'auditor' has to be capable of interpreting the solution and assessing the meeting of the standard. This may be early days, but early consideration of how 'good' can be measured will be key. Metrics for measuring solutions should also be non-channel specific, not just between technologies but also comparable against the more traditional methods of biometric comparisons e.g F2F. So one method of comparison could be the 'matching error rate' for the solution, which will help relying parties quantify their need and allow suppliers to grade their product. This will also allow technology to be compared with the human eye ball and challenge existing/dated standards, because at the time they were written the technology was poor/non existent.	See text	Noted

Comments Resolution on OASIS Biometric Open Protocol Specification (BOPS) Technical Committee (TC) draft charter

https://lists.oasis-open.org/archives/oasis-charter-discuss/201407/msg00000.html

Date: 07/23/2014	Document: **Comment Resolution BOPS TC**	Convenor Name Abbie Barbir

10		(1)(b) Statement of Purpose 1. What will be the benefits of using BOPS, compared to alternatives? For example, will it allow client software vendors interoperability between different server risk engines? (1)(c) Scope 2. API - programming language API or client/server protocol specification? Adding the term "client/server protocol specification" would ease my understanding. 3. REST, JSON, and Secure Socket Layers - This makes it easy to implement and maintain, but also have some drawbacks: We have recently seen weaknesses in SSL (most recently, Heartbleed), and relying on a single protocol for security might be risky. REST and JSON are easy to reverse engineer (and replace by a MITM) because of the string constants on the line. Possible countermeasures: * Adding a BOPS message encryption protocol on top of SSL would a) increase the security to make it secure also when the SSL implementation is compromised, and b) make it more difficult to reverse engineer the protocol. * Using ASN1/DER instead of JSON would avoid the string constants, requiring more effort to reverse engineer. * Requiring client signed messages is an option for avoiding substitution by a MITM. (1)(d) Deliverables 4. ... " prevents replay and the use of compromised devices." - To prevent the use of compromised devices can also be viewed as a risk decision to be taken by the risk engine. Suggest changing to "prevents replay and prevents/detects the use of compromised devices." Current application protection techniques typically use advanced obfuscated code to detect/prevent compromised device - this application protection code can also be reverse engineered and	See proposed text	Noted. Text improved.

		compromised, with some effort.		
11		I'm not sure I understand how wide in scope the BOPS will be. Will this include protocol specifications for all devices that may be used for biometric authentication (smartphones, and any other biometric capable collection and storage device)? Will this extend to servers, which may effectively broker the biometric information exchange? While OASIS will continue to work in parallel with FIDO, is there an intent to also work with the identity assurance frameworks..i.e. Kantara, Safe-Bio etc.? If so, how do you see these organizations complementing one another. Is it the intent for OASIS to come up with the technical specs and then have an organization like Kantara develop the associated policies around how this technology will be used for the varying levels of identity assurance? I'm sure I might have other questions at some point but wanted to at least get these over to you quickly given the deadline below. Again, I'm very interested in what is being contemplated here. I will also take a look at the OASIS membership categories and let you if this is something we are prepared to engage in.	See proposed text	Noted. All options are on the table. TC members can drive the direction of the TC.
12		[We are a] small company and we have concentrated over the last 10 years or so on developing IP associated with biometric authentication, particularly for mobile devices. During that time I have been involved with a number of Standards organizations and have contributed to a number of standards. At this point we are not prepared to join further standards organizations that charge dues. We do have patents and pending patents in the area and would ask that if your standards operate within the scope of these patents, that the practitioners of your standards take out a license under these patents. Alternatively if you would like to purchase the appropriate	See text	Noted. We do work within OASIS IPR rules. This is a TC and not a company.

		patents for you members, we can discuss that too.		
13		The idea is interesting and may have some practical use for us, though I think biometric authentication over the web is not a good idea for two reasons: - accuracy depends on the endpoint that collects the biometric information - finger print, iris scan etc., so it will be different from device to device. E.g. not all phones will have the same capabilities. - the collection device is too far from the authentication system. Sending biometric information over public internet is not a good idea. If password gets intercepted and compromised - it can be changed. The same cannot be done with biometrics.	See text	BOPS address your concerns and aims to protect identity related data
14		Sounds interesting. Do you have a unit cost per user on BOPS?	See text	Unit cost is zero. This will be a free protocol to implement.
15		I suggest you include in 1(c)Scope that the TC will review existing biometric security standards for discussion and potential referencing. For example, ANSI X9.84 - 2010, Biometric Information Management and Security has been published for many years and is currently beginning it's 5 Year Review. Much work went into this standard, with many participants, and it may give you a "shortcut" to drafting your standard.	See text	Noted. Text has been improved.
16		We are members of Fido, but it is not very relevant to what we are doing as we are not device dependent.	See text	Noted
17		I have to say that this initiative could be really interesting since remote matching is still a must for many of our costumers. Actually we have a solution for this specific use case which doesn´t follow any standard so far. After reading the proposal, I understand that the main goal is the creation of a standard protocol defining a complete procedure for completing enrollment and authentication tasks so that both security and privacy can be guaranteed		

		when matching is performed remotely on the server from a biometric sample captured on the device		
18		Quick question: do we give up any rights or ability to protect our intellectual property if we join?	See text	See OASIS IPR Policy. BOPS will be a non assert or an RF standard.
19		[* not anonymized since the source email message from Hector Hoyos was sent to principals/co-proposers, including: Jason Braverman; Scott Streit; Houda Kaddioui; Carolyn Flood, (work); Abbie Barbir; Eileen D Bridges; liz.votaw@bankofamerica.com; carol.geyer@oasis-open.org] I think it is very important that the BOPS framework: 1. Does not require tokens or if it allows them to be tokens which do NOT generate a private key, but rather have all private keys generated in the servers and sent to them. 2. Requires all data even in an underlying secure transfer layer to be further encrypted. 3. Does not allow user biometrics data to be stored in any back end repository, requiring the biometrics match to happen always on device, so as to protect the user's privacy as well as their data. 4. Requires the private key to be generated in a secure server behind a firewall and not on the device to avoid attacks that could lead to key factories being established. 5. Parse out information, distributing it in such a way that only indexes plus "minimal" (worthless to a hacker for their purpose) information are found in a repository, but all critical data is kept encrypted in the mobile device, effectively forcing hackers to hack a user at a time. Changing this paradigm will have a significant impact on deterring massive breaches of data. 7. Securing all access to back end repositories, servers, systems with mobile device based biometrics access.	None	noted

		8. Encrypting all information residing on a mobile device with minimum cypher requirements and linked to the user's biometrics. 9. I believe that it is important that we refer in the BOPS specifications to the standards set by NIST for accepted levels of image quality when acquiring an image for a biometrics, attaching such requirements to the BOPS-compliant process as well as require compliance with minimum sets of FRR (False rejection rates) and FAR (False Acceptance Rates) based on NIST averages stemming from their biometrics challenges. The rationale is that NIST has already invested significant amounts of time and resources over decades into all of this, so by simply requiring compliance with their standards we assure that it won't be "garbage in, garbage out" by anyone using any type of "fringe science" biometrics or something that has not been scientifically vetted by the appropriate community. 10. Requiring Liveness Detection Technology (LDT) to be deployed in conjunction with an Intrusion Detection System (IDS) on the device and back end. This will protect devices against spoofing. 11. Requiring IDS technology in the back end to monitor all systems and data traffic in all connected devices and servers in an environment. This is crucial because if not defending against Replay Attacks and Man In The Middle Attacks would be futile. I know that this is a "hot button" topic with some, but the reality is that living in the midst of the "Hacking Wars" era in which we find ourselves that is deteriorating by the day, we cannot afford to ignore this any longer. At Hoyos Labs we have developed technologies that comply with all of these requirements. Some folks accuse us of positioning ourselves in an unfair or preferential position vs other competitors of ours, because we came up with BOPS, as if we had any advantage. We don't. We could have		

		patented BOPS and not handed it over to IEEE or OASIS, but we did not. We did not because we believe that BOPS is a crucial framework that must be shared with all if we are to make any significant inroads in the "War Against Identities". For example, BOPS must require liveness detection technology to make sure biometrics are not spoofed. If it does not and devices are spoofed, then what good is it to secure a back end if we leave the front door open. At Hoyos Labs we developed a series of liveness detection systems that are proprietary, but as we did, many other companies can develop their own liveness detection systems too, and compete with us. We didn't say that BOPS LDT has to comply with X,Y, or Z criteria. We left it open so that the industry can come up with best of breed, and the same way that best of breed has established a series of NIST recognized standards in biometrics, some day the same will be true of BOPS LDT, but driven by the industry. This competition however must occur under a framework that protects all solutions and all consumers equally. Otherwise this is all an exercise in futility. This is applicable to very proposed rule of the framework. It is an open framework that everyone can build from and develop to for interoperability and just plain simple functionality.		
20		If we implement a BOPS solution, we would need to understand the unit cost, both initially and for on going support reasons. Definitions are broken down as follows: 1) Unit cost of a BOPS device - can range anywhere from $15 per unit to a high of $100 per unit. This would be a baseline. Let's use the $15/unit cost 2) Breakage - Normally we have to have a 10-20% pool available on hardware for re-supply. Due to the size/portability and industry turnover - go high at 20% 3) Training- training users on BOPS is similar to user/name password. Per user for setting up training/ documentation and certification - 15 minutes per person. Cost of training	See text	Not sure this is applicable. There is no charge to use BOPS. It will be a free standard to implement.

		$100 per hour. So for a unit cost, I would do the following: 100 site trial - 2 users per site on average. 200 (# of users) x $15 (unit cost) x breakage (1.2) + 200 (# of users) x $25 (hourly rate of training x training time. 200 x 15 x 1.2 + 200 x $25 = $8,600 or $43/unit to deploy. I still have to adjudicate the validation and turnover cost in order to understand the impact on the trial budget. I was looking to see if you had run the numbers on a use case (using your assumptions) so that we can understand the financial impact on the deployments.		