	Requirements Ordering			(snapshot taken	19 March 2017)
	Instructions:				
	0 - ONLY ONE RESPONSE PER ORGANIZATION 1 - duplicate the Ballot Template tab and rename it to your organization 1 - duplicate the Ballot Template tab and rename it to your organization				
	2 - place a 1 by each of the 10 most important requirements for your organization with respect to the data model spec 3 - please don't add to or edit any of the requirements				
	Plase condicts by 14 April 2017				
ID		(Org name)	,		
1	It must be obsible for any entity to issue a verifiable claim. (originally from UCR4.1)	(org name)			
2	It must be possible for the holder of a claim to restrict the amount of information exposed in a claim they choose to share. (originally from UCR4.2)				
3	It must be possible for the holder of a claim who chooses to share information in that claim to limit the duration for which that information is shared. (originally from				
	UCR4.2)				
4	It must be possible for an inspector to verify that the credential is an authentic statement of an issuer's claims about the subject. (originally from UCR4.3)				
5	The verifying entity must have the capability to connect the issuer's identity to its credential identifier and the subject's identity to their identifier as indicated in the credential. (orionially from UCR4.3)				
6	The issuer's verification information, such as its public key, must be discoverable from the credential record and verifiably linked to the issuer. (originally from UCR4.3)				
7	It must be possible to verify claims in an automated fashion. (originally from UCR4.3)				
8	It must be possible for the holder of a claim to store that claim in one or more credential repositories. (originally from UCR4.4)				
9	It must be possible for the holder to move a claim among credential repositories. (originally from UCR4.4)				
10	It must be possible for a holder to select if and which appropriate credential should be sent to an inspector. (originally from UCR4.5)				
11	It must be possible for the issuer of a claim to revoke it, after which it will no longer satisfy verification procedures. (originally from UCR4.6)				
12	The data model should be identifier agnostic (limiting to URIs is fine).				
13	The data model should be data syntax agnostic (should work in XML, JSON, CBUR, XDL, etc.)				
14	The data mixed should be signature suitable digitistic (should work with JVY), LDS, etc.). The data mixed should be extensible and composable in a decentralized way with strong machine-readable samatice (i.e. anyone can reach one userbulide target				
10	that can be used together with and will not collide with hersisting vocabularies without getting clearance from a centralized autohority or registry).				
16	It must be possible to express data in a way such that term collisions (key-value pairs) are guaranteed to not happen.				
17	It should be possible for an issuer to include data that is specific to that issuer in a way that guarantees no collisions when the data is merged with other claims.				
18	It should be possible to have digitally signed data at multiple levels of nesting.				
19	There should be a standard way to combine multiple sets of claims to produce a profile about a particular subject.				
20	It should be possible to express a revocation list for a particular set of claims.				
21	It should be possible to check a revocation list in a privacy-enhancing way (where the issuer cannot correlate the check, tor example).				
22	it should be possible to acquire privacy-enhancing single-use crecentulas rom a long-invice crecentula.				
23	it a notice to provide to information provide the determinance and south as a unique determinance information of the determinance association and the determinance information of the determinance and the determinance information of the determinance and the determinance information of the determinance and the determinance an				
24	It should be possible to countersign a credential (multi-sig support) and a profile of multiple credentials.				
25	It should be possible to add additional "endorsement" style signatures to a verifiable claim/credential/profile. It should be possible to "chain" these signatures, where each signature in the chain incorporates all of the previous ones in the chain.				
26	There should be some common vocabulary terms for expressing fundamentals such as the issuer, subject, etc.				
27	There should be a common vocabulary term for expressing alternative identifiers to enable delegation to issuing agents that may generate their own identifiers for or credentials (i.e. a piece of software may delegate the issuing of credentials to another agent and it should be possible for the software to express a unique identifier for that credential that is in a namespace the software manages and that may be a different identifier than the one the agent (or holder) assigns to the credential; note that this is not for origon-enhanced credential identifier use cases).				
28	It should be possible to counter-sign a credential or profile in a way that limits the usage of that credential or profile in a variety of ways, at a minimum, its usage at a narticular domain				
29	It should be possible for inspectors (or holders) to express how they intend to use credentials or profiles and for holders to counter-sign credentials or profiles with an acknowledgement/accentance of these terms				
30	It should be possible to express expiration periods (preferably validity periods i.e. start and expiration times).				
31	It should be possible to use the same data structure via an HTTP message, via a browser communication channel (postMessage, serviceWorker, etc.), and via Bluetooth.				
32	Be able to specify nature of attestment (native (i.e. Twitter attests that I'm @ChristopherA which they control) or confirm (Someone other than Twitter validates that I possess @ChristopherA at a particular time, but they don't control @ChristopherA)				
33	Proposal for Assertion, Evidence and Evaluation as per https://github.com/WebOfTrustInfo/portable-reputation-toolkit				
34	It should be possible for issuers to insert their usage policies into issued credentials. Policy rules include such things as: validity times, single/multiple usage, revocation info, inspector white or black lists, and any other rules that are understood by a community of credential stakeholders.				
35	Data objects, elements, and vocabulary terms in the data model should use or reference or align to existing standard vocabularies rather than create new definitions for common terms (e.g. Schema.org. CEDS. DCMI).				
36	Data objects, elements, and vocabulary terms should link to human-readable definitions, not just technical definitions with an assumed context, so non-technical audiences can understand what the data means.				
37	Any verifiable claim that represents a credential earned by a person or organization demonstrating competencies or performance tasks should link to standard definitions of those competencies using a structure like schema.org AlignmentObject https://schema.org/AlignmentObject. The target of each alignment may be machine-readable and human-readable definitions of the competency.				
38	The subject of the claim should be able to have the ability to refute the claim being made about them.				
39	It must be possible to publish a verifiable claim on an HTML Web Page such that a search engine can verify the authenticity of the information and index the information.				
40	It should be easy for a Web Developer to see (via view source or DOM inspection) what verifiable claims their website is publishing.				
41	It must be possible to extend the semantic meaning of verifiable claims without having to coordinate with a central repository.				
42	It should be possible to store credentials in a document-style/NoSQL or graph database without harming accessibility to the data or the ability to verify its authorship in				
	a siyimican way.				
	(Total points should be 10)	(	)		

Requirements Ordering						(snapshot taken 19 March 2017			
Instructions: 0 - ONLY OWE RESPONSE PER ORGANIZATION 1 - duplicate the Bailor Template tab and rename it to your organization 2 - place a 1 by each of the 10 most important requirements for your organization with respect to the data model spec 3 - please don't add to or edit any of the requirements									
Please complete by 14 April 2017	70	10	10	10	10	10	10	10	
ID Requirement Name	Count	Pearson	ETS	Digital Bazaar	uma.es	Univ Kent	Accreditrust	Legendary Re	
4 It must be possible for an inspector to verify that the credential is an authentic statement of an issuer's claims about the subject. (originally fr	m 7	1	1	1	1	1	1	1	
UCR4.3)	'		'	'		1	'	1	
11 It must be possible for the issuer of a claim to revoke it, after which it will no longer satisfy verification procedures. (originally from UCR4.6)	7	1	1	1	1	1	1	1	
1 It must be possible for any entity to issue a verifiable claim. (originally from UCR4.1)	5	1		1		1	1	1	
5 The verifying entity must have the capability to connect the issuer's identity to its credential identifier and the subject's identity to their identifier as indicated in the credential. (originally from UCR4.3)	fr 5		1	1	1	1	1		
6 The issuer's verification information, such as its public key, must be discoverable from the credential record and verifiably linked to the issue (orginally from UCPL 2)	5		1	1		1	1	1	
(Unginiary non OCH-3) 8. It must be possible for the holder of a claim to store that claim in one or more credential repositories. (originally from UCR4.4)	5	1	1	1		1	1		
The must be possible to verify claims in an automated fashion. (originally from LICP4.3)	4		1	1			1	1	
I it must be possible for a holder to select if and which approximate rendential should be sent to an inspector (originally from LICR4.5)	4	1	1			1		1	
It must be possible for the hold of select in and which appropriate determinal strong to serve to an inspection (originally information).	-								
UCR4.2) 4 The dispersion of the noder of a claim to restrict the amount of minimation exposed in a claim they choose to share, (originally nom UCR4.2)	3		1		1			1	
14 The data model should be signature scheme agrosuc (should work with jown, LDS, etc.)				1			1		
new vocabulary terms that can be used together with and will not collide with existing vocabularies without getting clearance from a centraliz authority or registry).	ed 3	1				1	1		
30 It should be possible to express expiration periods (preferably validity periods i.e. start and expiration times).	3	1			1		1		
3 It must be possible for the holder of a claim who chooses to share information in that claim to limit the duration for which that information is shared. (originally from UCR4.2)	2	1	1						
21 It should be possible to check a revocation list in a privacy-enhancing way (where the issuer cannot correlate the check, for example).	2				1			1	
41 It must be possible to extend the semantic meaning of verifiable claims without having to coordinate with a central repository.	2					1		1	
9 It must be possible for the holder to move a claim among credential repositories. (originally from UCR4.4)	1		1						
12 The data model should be identifier agnostic (limiting to URIs is fine).	1			1					
13 The data model should be data syntax agnostic (should work in XML, JSON, CBOR, XDI, etc.)	1			1					
17 It should be possible for an issuer to include data that is specific to that issuer in a way that guarantees no collisions when the data is merge with other claims.	1				1				
19 There should be a standard way to combine multiple sets of claims to produce a profile about a particular subject.	1							1	
25 It should be possible to add additional "endorsement" style signatures to a verifiable claim/credential/profile. It should be possible to "chain" these signatures, where each signature in the chain incorporates all of the previous ones in the chain.	1				1				
34 It should be possible for issuers to insert their usage policies into issued credentials. Policy rules include such things as: validity times, single/multiple usage, revocation info, inspector white or black lists, and any other rules that are understood by a community of credential stakeholders.	1					1			
35 Data objects, elements, and vocabulary terms in the data model should use or reference or align to existing standard vocabularies rather that create new definitions for common terms (e.g. Schema.org, CEDS, DCMI).	່ 1	1							
36 Data objects, elements, and vocabulary terms should link to human-readable definitions, not just technical definitions with an assumed conte so non-technical audiences can understand what the data means.	<sup>d,</sup> 1				1				
37 Any verhable claim that represents a credential earned by a person or organization demonstrating completences or performance tasks shoulink to standard definitions of those competencies using a structure like schema org AlignmentObject https://schema.org/AlignmentObject. TI target of each alignment may be machine-readable and human-readable definitions of the competency.	e 1				1				
16 It must be possible to express data in a way such that term collisions (key-value pairs) are guaranteed to not happen.	0								
18 It should be possible to have digitally signed data at multiple levels of nesting.	0								
20 It should be possible to express a revocation list for a particular set of claims.	0								
22 It should be possible to acquire privacy-enhancing single-use credentials from a long-lived credential.	0								
23 It should be possible to blind-sign portions of the credential data (such as a unique credential identifier) for certain use cases so that issuers cannot track usage even when inspectors collude with them.	0								
24 It should be possible to countersign a credential (multi-sig support) and a profile of multiple credentials.	0								
26 There should be some common vocabulary terms for expressing fundamentals such as the issuer, subject, etc.	0								
27 There should be a common vocabulary term for expressing alternative identifiers to enable delegation to issuing agents that may generate the own identifiers for credentials (i.e. a pice of software may delegate the issuing of credentials to another agent and it should be possible for software to express a unique identifier for that credential that is in a namespace the software manages and that may be a different identifier than the one the agent (or holder) assigns to the credential; no ole that this is no for privacy-enhanced credential identifier uses).	ne O								
28 It should be possible to counter-sign a credential or profile in a way that limits the usage of that credential or profile in a variety of ways, at a minimum, its usage at a particular domain.	0								
29 It should be possible for inspectors (or holders) to express how they intend to use credentials or profiles and for holders to counter-sign credentials or profiles with an acknowledgement/acceptance of these terms.	0								
31 It should be possible to use the same data structure via an HTTP message, via a browser communication channel (postMessage, serviceWorker, etc.), and via Bluetooth.	0								
32 Be able to specify nature of attestment (native (i.e. Twitter attests that I'm @ChristopherA which they control) or confirm (Someone other tha Twitter validates that I possess @ChristopherA at a particular time, but they don't control @ChristopherA)	0								
33 Proposal for Assertion, Evidence and Evaluation as per https://github.com/WebOfTrustInfo/portable-reputation-toolkit	0								
38 The subject of the claim should be able to have the ability to refute the claim being made about them.	0								
39 It must be possible to publish a verifiable claim on an HTML Web Page such that a search engine can verify the authenticity of the informatic and index the information.	0								
40 It should be easy for a Web Developer to see (via view source or DOM inspection) what verifiable claims their website is publishing.	0								
42 It should be possible to store credentials in a document-style/NoSQL or graph database without harming accessibility to the data or the abilit to verify its authorship in a significant way.	0								

	Requirements Ordering			(snapshot taken	19 March 2017)
	Instructions:				
	0 - ONLY ONE RESPONSE PER ORGANIZATION 1 - duplicate the Ballot Template tab and rename it to your organization 1				
	2 - place a 1 by each of the 10 most important requirements for your organization with respect to the data model spec 3 - places don't add to or edit any of the requirements				
	Please complete by 14 April 2017	10			
	Requirements Ordering	University of Mal	aga		
1	It must be possible for any entity to issue a vernable claim. (originally from UCH4.1)				
2	It must be possible for the holder of a claim to restrict the amount of information exposed in a claim they choose to share. (originally from UCR4.2)	1			
3	It must be possible for the holder of a claim who chooses to share information in that claim to limit the duration for which that information is shared. (originally from UCR4.2)				
4	It must be possible for an inspector to verify that the credential is an authentic statement of an issuer's claims about the subject. (originally from UCR4.3)	1			
5	The verifying entity must have the capability to connect the issuer's identity to its credential identifier and the subject's identity to their identifier as indicated in the credential. (originally from UCR4.3)	1			
6	The issuer's verification information, such as its public key, must be discoverable from the credential record and verifiably linked to the issuer. (originally from UCR4.3)				
7	It must be possible to verify claims in an automated fashion. (originally from UCR4.3)				
8	It must be possible for the holder of a claim to store that claim in one or more credential repositories. (originally from UCR4.4)				
9	It must be possible for the holder to move a claim among credential repositories. (originally from UCR4.4)				
10	It must be possible for a holder to select if and which appropriate credential should be sent to an inspector. (originally from UCR4.5)				
11	It must be possible for the issuer of a claim to revoke it, after which it will no longer satisfy verification procedures. (originally from UCR4.6)	1			
12	The data model should be identifier agnostic (limiting to URIs is fine).				
13	The data model should be data syntax agnostic (should work in XML, JSON, CBOR, XDI, etc.)				
14	The data model should be signature scheme agnostic (should work with JWT, LDS, etc.)				
15	The data model should be extensible and composable in a decentralized way with strong, machine-readable semantics (i.e. anyone can create new vocabulary terms that can be used together with and will not collide with existing vocabularies without getting clearance from a centralized authority or registry)				
16	It must be possible to express data in a way such that term collisions (key-value pairs) are quaranteed to not happen.				
17	It should be possible for an issuer to include data that is specific to that issuer in a way that guarantees no collisions when the data is merged with other claims.	1			
18	It should be possible to have digitally signed data at multiple levels of nesting.				
19	There should be a standard way to combine multiple sets of claims to produce a profile about a particular subject.				
20	It should be possible to express a revocation list for a particular set of claims.				
21	It should be possible to check a revocation list in a privacy-enhancing way (where the issuer cannot correlate the check, for example).	1			
22	It should be possible to acquire privacy-enhancing single-use credentials from a long-lived credential.				
23	It should be possible to blind-sign portions of the credential data (such as a unique credential identifier) for certain use cases so that issuers cannot track usage even when inspectrus collude with them				
24	It should be possible to countersion a credential (multi-sig support) and a profile of multiple credentials				
25	It should be possible to add additional "endorsement" style signatures to a verifiable claim/credential/profile. It should be possible to "chain" these signatures, where each signature in the chain incorporates all of the previous ones in the chain.	1			
26	each signature in the chain incorporates and or the previous ones in the chain. There should be some common vocaminary terms for averaging fundamentals such as the issuer subject at:				
27	There should be a common vocabulary term for excression alternative internatives to enable delenation to issuing agents that may generate their own identifiers for				
	credentials (i.e. a piece of software may delegate the issuing of credentials to another agent and it should be possible for the software to express a unique identifier for that credential that is in a namespace the software manages and that may be a different identifier than the one the agent (or holder) assigns to the credential; note that this is not for pirvacy-enhanced credential identifier use cases).				
28	It should be possible to counter-sign a credential or profile in a way that limits the usage of that credential or profile in a variety of ways, at a minimum, its usage at a particular domain.				
29	It should be possible for inspectors (or holders) to express how they intend to use credentials or profiles and for holders to counter-sign credentials or profiles with an acknowledgement/acceptance of these terms.				
30	It should be possible to express expiration periods (preferably validity periods i.e. start and expiration times).	1			
31	It should be possible to use the same data structure via an HTTP message, via a browser communication channel (postMessage, serviceWorker, etc.), and via Bluetooth.				
32	Be able to specify nature of attestment (native (i.e. Twitter attests that I'm @ChristopherA which they control) or confirm (Someone other than Twitter validates that I possess @ChristopherA at a particular time, but they don't control @ChristopherA)				
33	Proposal for Assertion, Evidence and Evaluation as per https://github.com/WebOfTrustInfo/portable-reputation-toolkit				
34	It should be possible for issuers to insert their usage policies into issued credentials. Policy rules include such things as: validity times, single/multiple usage, revocation info, inspector white or black lists, and any other rules that are understood by a community of credential stakeholders				
35	Data objects, elements, and vocabulary terms in the data model should use or reference or align to existing standard vocabularies rather than create new definitions for common terms (a or Schema are CEDS CMU)				
36	Data objects, elements, and vocabulary terms should link to human-readable definitions, not just technical definitions with an assumed context, so non-technical antidences and understand what the data means	1			
37	Any verifiable claim that represents a credential earned by a person or organization demonstrating competencies or performance tasks should link to standard definitions of those competencies using a structure like schema.org AlignmentObject https://schema.org/AlignmentObject. The target of each alignment may be machine.reachable and human.reachable definitions of the competency.	1			
38	The subject of the claim should be able to have the ability to reflue the claim being made about them.				
39	It must be possible to publish a verifiable claim on an HTMI. Web Page such that a search engine can verify the authenticity of the information and index the				
	information.				
40	It should be easy for a Web Developer to see (via view source or DOM inspection) what verifiable claims their website is publishing.				
41	It must be possible to extend the semantic meaning of verifiable claims without having to coordinate with a central repository.				
42	It should be possible to store credentials in a document-style/NoSQL or graph database without harming accessibility to the data or the ability to verify its authorship in a significant way.				
	(Total points should be 10)	10			

	Requirements Ordering			(snapshot taken	19 March 2017)
	Instructions:				
	0 - ONLY ONE RESPONSE PER ORGANIZATION 1 - duplicate the Bailot Template tab and rename it to your organization				
	2 - place a 1 by each of the 10 most important requirements for your organization with respect to the data model spec				
	Please complete by 14 April 2017	10			
ID	Requirements Ordering	(Org name)			
1	It must be possible for any entity to issue a verifiable claim. (originally from UCR4.1)	1			
2	It must be possible for the holder of a claim to restrict the amount of information exposed in a claim they choose to share. (originally from UCR4.2)				
3	It must be possible for the holder of a claim who chooses to share information in that claim to limit the duration for which that information is shared. (originally from UCR4.2)				
4	It must be possible for an inspector to verify that the credential is an authentic statement of an issuer's claims about the subject. (originally from UCR4.3)	1			
5	The verifying entity must have the capability to connect the issuer's identity to its credential identifier and the subject's identity to their identifier as indicated in the	1			
	credential. (originally from UCR4.3)				
6	The issuer's verification information, such as its public key, must be discoverable from the credential record and verifiably linked to the issuer. (originally from UCR4.3)	1			
1	It must be possible to verify claims in an automated fashion. (orginally from UCR4.3)				
8	It must be possible for the holder of a claim to store that claim in one or more credential repositories. (originally from UCR4.4)	1			
9	It must be possible for the houser to move a claim among recentual repositories. (originality from UCK4.4) If must be possible for a bidget to select if and which appropriate credential should be sent to an inspectrum (originality from UCR4.5)	1			
11	it must be possible for a notice to seleculity and which appropriate developing is not to easily for inspective (inspective) (inspectiv	1			
12	It made to positive for the sector of a claim to revolve it, and which renders addry comparison procedures, (originary non-convex.) The data model should be identifier agnostic (limiting to IRIs is fine)				
13	The data model should be data syntax agnostic (should work in XML JSON, CBOR, XDI, etc.)				
14	The data model should be signature scheme agnostic (should work with JWT, LDS, etc.)				
15	The data model should be extensible and composable in a decentralized way with strong, machine-readable semantics (i.e. anyone can create new vocabulary terms	1			
	that can be used together with and will not collide with existing vocabularies without getting clearance from a centralized authority or registry).				
16	It must be possible to express data in a way such that term collisions (key-value pairs) are guaranteed to not happen.				
17	It should be possible for an issuer to include data that is specific to that issuer in a way that guarantees no collisions when the data is merged with other claims.				
18	It should be possible to have digitally signed data at multiple levels of nesting.				
19	There should be a standard way to combine multiple sets of claims to produce a profile about a particular subject.				
20	It should be possible to express a revocation list for a particular set of clarins.				
21	in should be possible to check a revolution is in a phracy-enhancing way (where the issuer cannot contrate the check, for example).				
23	is anotable possible to begane privacy emanantial angle-ose encountiants more a conjunce executional.				
20	when inspectors collude with them.				
24	It should be possible to countersign a credential (multi-sig support) and a profile of multiple credentials.				
25	It should be possible to add additional "endorsement" style signatures to a verifiable claim/credential/profile. It should be possible to "chain" these signatures, where each signature in the chain incorporates all of the previous ones in the chain.				
26	There should be some common vocabulary terms for expressing fundamentals such as the issuer, subject, etc.				
27	There should be a common vocabulary term for expressing alternative identifiers to enable delegation to issuing agents that may generate their own identifiers for				
	that credential that is in a namespace the software manages and that may be a different identifier than the one the agent (or holder) assigns to the credential; note that this is not invariant and it should be possible for the software to express a unique identifier to that the one the agent (or holder) assigns to the credential; note that this is not find the find the find the find the credential; note that this is not find the find the credential; note that the one the agent (or holder) assigns to the credential; note that this is not find the find the credential; note that the cre				
28	us is not to prove the example interview of the end of				
20	particular domain.				
20	a shade be possible on inspectors (or inspector of these terms.) acknowledgement/acceptance of these terms. I should be possible to express exprisition product (areferable unliftly possible in a fast and expiration times)				
31	is should be possible to use the same data structure via an HTTP messare via a browser communication channel (nostMessare serviceWorker etc.) and via				
22	Roman of possible of dealer of the dealer of				
32	De aue to speciny name or aucoment (name (t.e. ninute aucos) and in gerinsophen which are control or continuin (conteche other than livitter validates that i possess @ChristopherA at a particular time, but they don't control @ChristopherA				
33	Proposal for Assertion, Evidence and Evaluation as per https://github.com/web/Urinstithub/portable-reputation-toolkit H chauld be preclade the used to be precladed by the used and precladed by the land of the land of the used to be the used of t				
34	It should be possible for issuers to insert their usage policies into issued credentials. Policy rules include such things as: validity times, single/multiple usage, revocation info, inspector white or black lists, and any other rules that are understood by a community of credential stakeholders.	1			
35	Data objects, elements, and vocabulary terms in the data model should use or reference or align to existing standard vocabularies rather than create new definitions for common terms (e.g. Schema.org, CEDS, DCMI).				
36	Data objects, elements, and vocabulary terms should link to human-readable definitions, not just technical definitions with an assumed context, so non-technical audiences can understand what the data means.				
37	Any verifiable claim that represents a credential earned by a person or organization demonstrating competencies or performance tasks should link to standard definitions of those competencies using a structure like schema org AlignmentObject https://schema.org/AlignmentObject. The target of each alignment may be machine-readable and human-readable definitions of the competency.				
38	The subject of the claim should be able to have the ability to refute the claim being made about them.				
39	It must be possible to publish a verifiable claim on an HTML Web Page such that a search engine can verify the authenticity of the information and index the information.				
40	It should be easy for a Web Developer to see (via view source or DOM inspection) what verifiable claims their website is publishing.				
41	It must be possible to extend the semantic meaning of verifiable claims without having to coordinate with a central repository.	1			
42	It should be possible to store credentials in a document-style/NoSQL or graph database without harming accessibility to the data or the ability to verify its authorship in a significant way.				
	(Total points should be 10)	10			

	Requirements Ordering			(snapshot taken	19 March 2017)
	Instructions:				
	0 - ONLY ONE RESPONSE PER ORGANIZATION 1- duplicate the Ballot Template tab and rename it to your organization 1-				
	2 - place a 1 by each of the 10 most important requirements for your organization with respect to the data model spec 3 - please don't add to or edit any of the requirements				
	Blance complete by 14 April 2017	10			
ID		10 A core ditruct			
1	Requirements ordering If must be possible for any entity to issue a verifiable claim (originally from LICR4.1)	1			
2	It must be possible for the holder of a claim to restrict the amount of information exposed in a claim they choose to share. (originally from UCR4.2)				
3	It must be possible for the holder of a claim who chooses to share information in that claim to limit the duration for which that information is shared. (originally from				
	UCR4.2)				
4	It must be possible for an inspector to verify that the credential is an authentic statement of an issuer's claims about the subject. (originally from UCR4.3)	1			
5	The verifying entity must have the capability to connect the issuer's identity to its credential identifier and the subject's identity to their identifier as indicated in the credential. (originally from UCR4.3)	1			
6	The issuer's verification information, such as its public key, must be discoverable from the credential record and verifiably linked to the issuer. (originally from UCR4.3)	1			
7	It must be possible to verify claims in an automated fashion. (originally from UCR4.3)	1			
8	It must be possible for the holder of a claim to store that claim in one or more credential repositories. (originally from UCR4.4)	1			
9	It must be possible for the holder to move a claim among credential repositories. (originally from UCR4.4)				
10	It must be possible for a holder to select if and which appropriate credential should be sent to an inspector. (originally from UCR4.5)				
11	It must be possible for the issuer of a claim to revoke it, after which it will no longer satisfy verification procedures. (originally from UCR4.6)	1			
12	The data model should be identifier agnostic (limiting to URIs is fine).				
13	The data model should be data syntax agnostic (should work in XML, JSON, CBOR, XDI, etc.)				
14	The data model should be signature scheme agnostic (should work with JWT, LDS, etc.)	1			
15	The data model should be extensible and composable in a decentralized way with strong, machine-readable semantics (i.e. anyone can create new vocabulary terms that can be used together with and will not collide with existing vocabularies without getting clearance from a centralized authority or registry).	1			
16	It must be possible to express data in a way such that term collisions (key-value pairs) are guaranteed to not happen.				
17	It should be possible for an issuer to include data that is specific to that issuer in a way that guarantees no collisions when the data is merged with other claims.				
18	It should be possible to have digitally signed data at multiple levels of nesting.				
19	There should be a standard way to combine multiple sets of claims to produce a profile about a particular subject.				
20	It should be possible to express a revocation list for a particular set of claims.				
21	It should be possible to check a revocation list in a privacy-enhancing way (where the issuer cannot correlate the check, for example).				
22	It should be possible to acquire privacy-enhancing single-use credentials from a long-lived credential.				
23	It should be possible to blind-sign portions of the credential data (such as a unique credential identifier) for certain use cases so that issuers cannot track usage even when inspectors collude with them.				
24	It should be possible to countersign a credential (multi-sig support) and a profile of multiple credentials.				
25	It should be possible to add additional "endorsement" style signatures to a verifiable claim/credential/profile. It should be possible to "chain" these signatures, where each signature in the chain incorporates all of the previous ones in the chain.				
26	There should be some common vocabulary terms for expressing fundamentals such as the issuer, subject, etc.				
27	There should be a common vocabulary term for expressing alternative identifiers to enable delegation to issuing agents that may generate their own identifiers for credentials (i.e. a piece of enhance may delegate the issuing of credentials to another agent and it should be possible for the software to express a unique identifier for				
	that credential that is in a namespace the software manages and that may be a different identifier than the one the agent (or holder) assigns to the credential, note that this is not for privacy-enhanced credential identifier use cases).				
28	It should be possible to counter-sign a credential or profile in a way that limits the usage of that credential or profile in a variety of ways, at a minimum, its usage at a				
29	It should be possible for inspectors (or holders) to express how they intend to use credentials or profiles and for holders to counter-sign credentials or profiles with an				
30	acknowledgement/acceptance of these terms. It should be possible to express expiration periods (preferably validity periods i.e. start and expiration times).	1			
31	It should be possible to use the same data structure via an HTTP message, via a browser communication channel (postMessage, serviceWorker, etc.), and via Bluetooth.				
32	Be able to specify nature of attestment (native (i.e. Twitter attests that I'm @ChristopherA which they control) or confirm (Someone other than Twitter validates that I nosees @ChristopherA at a particular time, but they don't control @ChristopherA				
33	Proposal for Assertion, Evidence and Evaluation as per https://divence.org/evaluation.com/evaluation/control/evaluatio				
34	It should be possible for issuers to insert their usage policies into issued credentials. Policy rules include such things as: validity times, single/multiple usage,				
35	revocation info, inspector white or black lists, and any other rules that are understood by a community of credential stakeholders. Data objects, elements, and vocabulary terms in the data model should use or reference or align to existing standard vocabularies rather than create new definitions				
36	for common terms (e.g. Schema.org, CEDS, DCMI). Data objects elements and vocabulary terms should link to human-readable definitions on inst technical definitions with an assumed context, so non-technical				
00	audiences can understand what the data means.				
31	Any verinaure camman represense a usedential earned by a person or organization demonstrating competencies or performance tasks should link to standard definitions of those competencies using a structure like schema org AlignmentObject https://schema.org/AlignmentObject. The target of each alignment may be machine-readable and human-readable definitions of the competency.				
38	The subject of the claim should be able to have the ability to refute the claim being made about them.				
39	It must be possible to publish a verifiable claim on an HTML Web Page such that a search engine can verify the authenticity of the information and index the information.				
40	It should be easy for a Web Developer to see (via view source or DOM inspection) what verifiable claims their website is publishing.				
41	It must be possible to extend the semantic meaning of verifiable claims without having to coordinate with a central repository.				
42	It should be possible to store credentials in a document-style/NoSQL or graph database without harming accessibility to the data or the ability to verify its authorship in a significant way.				
	(Total points should be 10)	10			

	Requirements Ordering				
	0 - OVELT ONE RESPONSE FER VICENTIAN     1- duplicate the Ballot Template tab and rename it to your organization     2- place a 1-by each of the 31-by most important requirements for your organization				
	3 - please don't add to or edit any of the requirements				
	Please complete by 14 April 2017	10			
ID	Requirements Ordering	Pearson			
4	It must be possible for an inspector to verify that the credential is an authentic statement of an issuer's claims about the subject (originally from LICR4.3)	1			
8	It must be possible for the holder of a claim to store that claim in one or more credential repositories. (originally from UCR4.4)	1			
11	It must be possible for the issuer of a claim to revoke it, after which it will no longer satisfy verification procedures. (originally	1			
	from UCR4.6)				
1	It must be possible for any entity to issue a verifiable claim. (originally from UCR4.1)	1			
2	It must be possible for the holder of a claim to restrict the amount of information exposed in a claim they choose to share. (originally from UCR4.2)				
3	It must be possible for the holder of a claim who chooses to share information in that claim to limit the duration for which that information is shared (originally from LICR4.2).	1			
5	The verifying entity must have the capability to connect the issuer's identity to its credential identifier and the subject's identity to their identifier as indicated in the credential (originally from LICP4.3)				
10	It must be possible for a holder to select if and which appropriate credential should be sent to an inspector. (originally from	1			
14	The data model should be signature scheme agnostic (should work with JWT LDS, etc.)	1			
15	The data model should be extensible and composable in a decentralized way with strong, machine-readable semantics (i.e.				
	anyone can create new vocabulary terms that can be used together with and will not collide with existing vocabularies without getting clearance from a centralized authority or registry).	1			
21	It should be possible to check a revocation list in a privacy-enhancing way (where the issuer cannot correlate the check, for example).				
30	It should be possible to express expiration periods (preferably validity periods i.e. start and expiration times).	1			
6	The issuer's verification information, such as its public key, must be discoverable from the credential record and verifiably linked to the issuer (originally from LICR4.3)				
7	It must be possible to verify claims in an automated fashion, (originally from UCR4.3)				
9	It must be possible for the holder to move a claim among credential repositories. (originally from UCR4.4)				
12	The data model should be identifier agnostic (limiting to URIs is fine).				
13	The data model should be data syntax agnostic (should work in XML, JSON, CBOR, XDI, etc.)				
17	It should be possible for an issuer to include data that is specific to that issuer in a way that guarantees no collisions when the data is merced with other claims.				
19	There should be a standard way to combine multiple sets of claims to produce a profile about a particular subject.				
25	It should be possible to add additional "endorsement" style signatures to a verifiable claim/credential/profile. It should be				
	possible to "chain" these signatures, where each signature in the chain incorporates all of the previous ones in the chain.				
31	It should be possible to use the same data structure via an HTTP message, via a browser communication channel (postMessage, serviceWorker, etc.), and via Bluetooth.				
35	Data objects, elements, and vocabulary terms in the data model should use or reference or align to existing standard vocabularies rather than create new definitions for common terms (e.g. Schema.org, CEDS, DCMI).	1			
36	Data objects, elements, and vocabulary terms should link to human-readable definitions, not just technical definitions with an assumed context, so non-technical audiences can understand what the data means.				
37	Any verifiable claim that represents a credential earned by a person or organization demonstrating competencies or performance tasks should link to standard definitions of those competencies using a structure like schema.org AlignmentObject https://schema.org/AlignmentObject. The target of each alignment may be machine-readable and human- roadable deficience of the competencies.				
41	It must be possible to extend the semantic meaning of verifiable claims without having to coordinate with a central repository				
16	It must be possible to express data in a way such that term collisions (key-value pairs) are guaranteed to not happen.				
18	It should be possible to have digitally signed data at multiple levels of nesting.				
20	It should be possible to express a revocation list for a particular set of claims.				
22	It should be possible to acquire privacy-enhancing single-use credentials from a long-lived credential.				
23	It should be possible to blind-sign portions of the credential data (such as a unique credential identifier) for certain use cases so that issuers cannot track usage even when inspectors collude with them				
24	It should be possible to countersign a credential (multi-sig support) and a profile of multiple credentials				
26	There should be some common vocabulary terms for expressing fundamentals such as the issuer, subject, etc.				
27	There should be a common vocabulary term for expressing alternative identifiers to enable delegation to issuing agents that may generate their own identifiers for credentials (i.e. a piece of software may delegate the issuing of credentials to another agent and it should be possible for the software to express a unique identifier for that credential that is in a namespace the software manages and that may be a different identifier than the one the agent (or holder) assigns to the credential; note that this is not for oursecuend paradert identifier use cases).				
28	It should be possible to counter-sign a credential or profile in a way that limits the usage of that credential or profile in a variety of ways, at a minimum, its usage at a particular domain.				
29	It should be possible for inspectors (or holders) to express how they intend to use credentials or profiles and for holders to counter-sion credentials or profiles with an acknowledgement/acceptance of these terms.				
32	Be able to specify nature of attestment (native (i.e. Twitter attests that I'm @ChristopherA which they control) or confirm (Someone other than Twitter validates that I possess @ChristopherA at a particular time, but they don't control @ChristopherA)				
33	Proposal for Assertion. Evidence and Evaluation as per https://oithub.com/WebOfTrustInfo/portable-reputation-toolkit				
34	It should be possible for issuers to insert their usage policies into issued credentials. Policy rules include such things as:				
	validity times, single/multiple usage, revocation info, inspector white or black lists, and any other rules that are understood by a community of credential stakeholders.				
38	The subject of the claim should be able to have the ability to refute the claim being made about them.				
39	It must be possible to publish a verifiable claim on an HTML Web Page such that a search engine can verify the authenticity of the information and index the information				
40	It should be easy for a Web Developer to see (via view source or DOM inspection) what verifiable claims their website is nublishing				
42	It should be possible to store credentials in a document-style/NoSQL or graph database without harming accessibility to the				
	data or the ability to verify its authorship in a significant way.				
	(Total points should be 10)	10			

				(an analy at talian	40 Marsh 2017)
	Requirements Ordering			(snapsnot taken	19 March 2017)
	Instructions: 0 - ONLY ONE RESPONSE PER ORGANIZATION				
	1 - duplicate the Ballot Template tab and rename it to your organization				
	2 - place all by each or the 10 most important requirements for your organization with respect to the data model spec 3 - place down and to or edit any of the requirements				
	Blooce complete by 44 Andl 2017				
	Press Complete by the April 2017	10			
0	Requirements of company	EIS			
	ti must be possible for any emitty to issue a verifiable carm. (originally from OCK4.1)				
2	It must be possible for the holder of a claim to restrict the amount of information exposed in a claim trey choose to share. (orginally from OCR4.2)				
3	ternos de possible foi de noteel or a claim who choses to share information in that claim to innut the duration for which that information is shared. (originally norm UCR4.2)				
4	It must be possible for an inspector to verify that the credential is an authentic statement of an issuer's claims about the subject. (originally from UCR4.3)	1			
5	The verifying entity must have the capability to connect the issuer's identity to its credential identifier and the subject's identity to their identifier as indicated in the	1			
	credential. (originally from UCR4.3)				
6	The issuer's verification information, such as its public key, must be discoverable from the credential record and verifiably linked to the issuer. (originally from UCR4.3)	1			
7	It must be possible to verify claims in an automated fashion. (originally from UCR4.3)	1			
8	It must be possible for the holder of a claim to store that claim in one or more credential repositories. (originally from UCR4.4)	1			
9	It must be possible for the holder to move a claim among credential repositories. (originally from UCR4.4)	1			
10	It must be possible for a holder to select if and which appropriate credential should be sent to an inspector. (originally from UCR4.5)	1			
11	It must be possible for the issuer of a claim to revoke it, after which it will no longer satisfy ventication procedures. (originally from UCR4.6)	1			
12	The data model should be identifier agnostic (limiting to URIs is tine).				
13	The data inicide should be data syntax agnostic (should work in XML, JSON, CBUK, XUL, etc.)				
14	The data microer should be signature scheme agnostic (should work with JW), LUS, etc.)				
10	The data index should be exensible and composable in a decentralized way with strong, machine-leadable semantics (i.e. allyone can create new Vocabulary terms that can be used together with and will not collide with existing vocabularies without getting clearance from a centralized authority or registry).				
16	It must be possible to express data in a way such that term collisions (key-value pairs) are guaranteed to not happen.				
17	It should be possible for an issuer to include data that is specific to that issuer in a way that guarantees no collisions when the data is merged with other claims.				
18	It should be possible to have digitally signed data at multiple levels of nesting.				
19	There should be a standard way to combine multiple sets of claims to produce a profile about a particular subject.				
20	It should be possible to express a revocation list for a particular set of claims.				
21	It should be possible to check a revocation list in a privacy-enhancing way (where the issuer cannot correlate the check, for example).				
22	It should be possible to acquire privacy-enhancing single-use credentials from a long-lived credential.				
23	It should be possible to blind-sign portions of the credential data (such as a unique credential identifier) for certain use cases so that issuers cannot track usage even				
~ *	when inspectors collude with them.				
24	it snould be possible to countersign a credential (multi-sig support) and a profile of multiple credentials.				
25	It should be possible to add additional 'endorsement' style signatures to a verinable claim/credential/prome. It should be possible to 'chain' these signatures, where each signature in the chain incorporates all of the previous ones in the chain.				
26	There should be some common vocabulary terms for expressing fundamentals such as the issuer, subject, etc.				
27	There should be a common vocabulary term for expressing alternative identifiers to enable delegation to issuing agents that may generate their own identifiers for				
	credentials (i.e. a piece of software may delegate the issuing of credentials to another agent and it should be possible for the software to express a unique identifier for				
	that credential that is in a namespace the software manages and that may be a different identifier than the one the agent (or noider) assigns to the credential; note that this is not for privacy-enhanced credential identifier use cases).				
28	It should be possible to counter-sign a credential or profile in a way that limits the usage of that credential or profile in a variety of ways, at a minimum, its usage at a				
	particular domain.				
29	It should be possible for inspectors (or holders) to express how they intend to use credentials or profiles and for holders to counter-sign credentials or profiles with an acknowledgescaptionspace these to prove the terms of the second sec				
20	acknowledgemenuacceptance of unese terms.				
31	it should be possible to express expration periods (preferance value) periods to stati and expration innes). If should be possible to use the same data churching value y value y periods to stati and expration innes).				
31	n anown de possione to dee the sente data suddate via an miner message, via a browset communication chaminer (postmessage, selvice worker, etc.), and via Bluetooth.				
32	Be able to specify nature of attestment (native (i.e. Twitter attests that I'm @ChristopherA which they control) or confirm (Someone other than Twitter validates that I				
	possess @ChnstopherA at a particular time, but they don't control @ChristopherA)				
33	Proposal ion Assertion, E-vidence and E-valuation as per https://gitnub.com/web/ir institution/portable-reputation-toolkit				
34	It snoulu be possible for issuers to insert their usage policies into issued credentials. Policy rules include such things as: validity times, single/multiple usage, revocation info, inspector white or black lists, and any other rules that are understood by a community of credential stakeholders.				
35	Data objects, elements, and vocabulary terms in the data model should use or reference or align to existing standard vocabularies rather than create new definitions				
	for common terms (e.g. Schema.org, CEDS, DCMI).				
36	Data objects, elements, and vocabulary terms should link to human-readable definitions, not just technical definitions with an assumed context, so non-technical				
27	audiences can understand what the data means.				
3/	Any remove view in the represente a credential earlied by a person or organization enconstraing competencies or periorinance tasks should link to standard definitions of those competencies using a structure like schema.org/AlignmentObject https://schema.org/AlignmentObject. The target of each alignment may be				
	machine-readable and human-readable definitions of the competency.				
38	The subject of the claim should be able to have the ability to refute the claim being made about them.				
39	It must be possible to publish a verifiable claim on an HTML Web Page such that a search engine can verify the authenticity of the information and index the				
40	intermediate.				
41	It must be possible to extend the semantic meaning of verifiable claims without having to coordinate with a central repository				
42	It should be possible to store credentials in a document-style/NoSQL or graph database without harming accessibility to the data or the ability to verify its authorshin in				
	a significant way.				
	(Total points should be 10)	10			

	Requirements Ordering			(snapshot taken	19 March 2017)
	Instructions:				
	0 - ONLY ONE RESPONSE PER ORGANIZATION 1 - duplicate the Ballot Template tab and rename it to your organization 1				
	2 - place a 1 by each of the 10 most important requirements for your organization with respect to the data model spec 3 - places don's dath or certification with respiration memory and the spect of the data model spect and the spect of the spece of the spect of the spect of the spect of the				
	Please complete by 14 April 2017	10			
ID	Requirements Ordering	Digital Bazaar			
1	It must be possible for any entity to issue a verifiable claim. (originally from UCR4.1)	1			
2	It must be possible for the holder of a claim to restrict the amount of information exposed in a claim they choose to share. (originally from UCR4.2)				
3	It must be possible for the holder of a claim who chooses to share information in that claim to limit the duration for which that information is shared. (originally from UCR4.2) UCR4.2)				
4	It must be possible for an inspector to verify that the credential is an authentic statement of an issuer's claims about the subject. (originally from UCR4.3)	1			
5	The verifying entity must have the capability to connect the issuer's identity to its credential identifier and the subject's identity to their identifier as indicated in the credential (originally from UCR4.3)	1			
6	The issuer's verification information, such as its public key, must be discoverable from the credential record and verifiably linked to the issuer. (originally from UCR4.3)	1			
7	It must be possible to verify claims in an automated fashion. (originally from UCR4.3)	1			
8	It must be possible for the holder of a claim to store that claim in one or more credential repositories. (originally from UCR4.4)	1			
9	It must be possible for the holder to move a claim among credential repositories. (originally from UCR4.4)				
10	It must be possible for a holder to select if and which appropriate credential should be sent to an inspector. (originally from UCR4.5)				
11	It must be possible for the issuer of a claim to revoke it, after which it will no longer satisfy verification procedures. (originally from UCR4.6)	1			
12	The data model should be identifier agnostic (limiting to URIs is fine).	1			
13	The data model should be data syntax agnostic (should work in XML, JSON, CBOR, XDI, etc.)	1			
14	The data model should be signature scheme agnostic (should work with JWT, LDS, etc.)	1			
15	The data model should be extensible and composable in a decentralized way with strong, machine-readable semantics (i.e. anyone can create new vocabulary terms				
10	that can be used together with and will not collide with existing vocabularies without getting clearance from a centralized authority or registry).				
10	It must be possible to express data in a way such that term constants (key-value pairs) are guaranteed to not happen.				
10	It should be possible for an issue to include data that is specific to that issuer in a way that guarantees no consisting when the data is merged with other claims. It should be possible to an issuer to include data that is specific to that issuer and way that guarantees no consisting when the data is merged with other claims.				
10	it should be actually signed data at multiple reversion results.				
20	There should be a standard way to combine multiple sets or claims to produce a police about a particular subject.				
20	It should be possible to exploses a revocation list for a particular set of claims.				
21	It should be possible to check a revolution its in a prody-enhanced with the issuer cannot contrate the check, for example).				
23	is should be possible to Bundler privacy of manying single-bac decompanies income a registrice decompanies of the contract of the should be possible to blind-kinn provides of the randomital data (such as a unique predential idantifier) for cartain use passes on that issuare cannot track usane avan				
20	trained be possible to minimise any posterior or the orderinan data (seen as a binque orderinan demand) for extrain data data so a mot radia dage even when inspectors collude with them.				
24	It should be possible to countersign a credential (multi-sig support) and a profile of multiple credentials.				
25	It should be possible to add additional "endorsement" style signatures to a verifiable claim/credential/profile. It should be possible to "chain" these signatures, where each signature in the chain incorporates all of the previous ones in the chain.				
26	There should be some common vocabulary terms for expressing fundamentals such as the issuer, subject, etc.				
27	There should be a common vocabulary term for expressing alternative identifiers to enable delegation to issuing agents that may generate their own identifiers for				
	credentials (i.e. a piece of software may delegate the issuing of credentials to another agent and it should be possible for the software to express a unique identifier for that credential that is in a namespace the software manages and that may be a different identifier than the one the agent (or holder) assigns to the credential; note that this is not for orivacy-enhanced credential identifier use cases).				
28	It should be possible to counter-sign a credential or profile in a way that limits the usage of that credential or profile in a variety of ways, at a minimum, its usage at a				
29	particular outman. It should be possible for inspectors (or holders) to express how they intend to use credentials or profiles and for holders to counter-sign credentials or profiles with an extravaledneem/loccentance of these terms				
30	It should be possible to express expiration periods (preferably validity periods i.e. start and expiration times).				
31	It should be possible to use the same data structure via an HTTP message, via a browser communication channel (postMessage, serviceWorker, etc.), and via				
32	Be able to specify nature of attestment (native (i.e. Twitter attests that I'm @ChristopherA which they control) or confirm (Someone other than Twitter validates that I				
33	possess @UninstopnerA at a particular time, but they don't control @UninstopnerA) Proposal for Assertion. Evidence and Evaluation as per https://github.com/WebOTrustInfo/portable-reputation-toolkit				
34	It should be possible for issuers to insert their usage policies into issued credentials. Policy rules include such things as: validity times, single/multiple usage.				
35	revocation info, inspector white or black lists, and any other rules that are understood by a community of credential stakeholders.				
	for common terms (e.g. Schema.org, CEDS, DCMI).				
36	Data objects, elements, and vocabulary terms should link to human-readable definitions, not just technical definitions with an assumed context, so non-technical audiences can understand what the data means.				
37	Any verifiable claim that represents a credential earned by a person or organization demonstrating competencies or performance tasks should link to standard definitions of those competencies using a structure like schema.org AlignmentObject https://schema.org/AlignmentObject. The target of each alignment may be machine-readable and human-readable definitions of the competency.				
38	The subject of the claim should be able to have the ability to refute the claim being made about them.				
39	It must be possible to publish a verifiable claim on an HTML Web Page such that a search engine can verify the authenticity of the information and index the information				
40	It should be easy for a Web Developer to see (via view source or DOM inspection) what verifiable claims their website is publishing.				
41	It must be possible to extend the semantic meaning of verifiable claims without having to coordinate with a central repository.				
42	It should be possible to store credentials in a document-style/NoSQL or graph database without harming accessibility to the data or the ability to verify its authorship in				
	a significant way.				
	(Total points should be 10)	10			

	Requirements Ordering				(snapshot taken	19 March 2017)
	Instructions:					
	0 - ONLY ONE RESPONSE PER ORGANIZATION 1- duplicate the Ballot Template tab and rename it to your organization 1-					
	2 - place a 1 by each of the 10 most important requirements for your organization with respect to the data model spec 3 - please don't add to or edit any of the requirements					
	Hease complete by 14 April 2017	10		1.1		
	Requirements Ordering	Legendary Requ	irements (Joe And	drieu)		
1	It must be possible for any entity to issue a vernable daim. (originally from UCK4.1)	1				
2	It must be possible for the holder of a claim to restrict the amount or information exposed in a claim they choose to share. (originally from UCR4.2)	1				
3	It must be possible for the holder of a claim who chooses to share information in that claim to infinit the duration for which that information is shared. (originally non- UCR4.2)					
4	It must be possible for an inspector to verify that the credential is an authentic statement of an issuer's claims about the subject. (originally from UCR4.3)	1				
5	The verifying entity must have the capability to connect the issuer's identity to its credential identifier and the subject's identity to their identifier as indicated in the					
6	decentral. (originally non oces.)	1				
7	The issue's residual metalion metalion such as the public of discontration of the instance of the issue's (originally more of	1				
8	It must be possible for the holder of a claim to store that claim in one or more credential representative (originally from LICP4.4)					
9	It must be possible for the holder to move a claim among credential repositories. (originally from UCR4.4)					
10	It must be possible for a bolder to select if and which appropriate repeations. (organity from to an inspector (originally from UCR4.5)	1				
11	It must be possible for the issuer of a claim to revoke it after which it will no longer satisfy verification procedures. (priorially from UCR4.6)	1				
12	The data model should be identifier agnostic (limiting to URIs is fine).					
13	The data model should be data syntax agnostic (should work in XML, JSON, CBOR, XDI, etc.)					
14	The data model should be signature scheme agnostic (should work with JWT, LDS, etc.)					
15	The data model should be extensible and composable in a decentralized way with strong, machine-readable semantics (i.e. anyone can create new vocabulary terms					
	that can be used together with and will not collide with existing vocabularies without getting clearance from a centralized authority or registry).					
16	It must be possible to express data in a way such that term collisions (key-value pairs) are guaranteed to not happen.					
17	It should be possible for an issuer to include data that is specific to that issuer in a way that guarantees no collisions when the data is merged with other claims.					
18	It should be possible to have digitally signed data at multiple levels of nesting.					
19	There should be a standard way to combine multiple sets of claims to produce a profile about a particular subject.	1				
20	It should be possible to express a revocation list for a particular set of claims.					
21	It should be possible to check a revocation list in a privacy-enhancing way (where the issuer cannot correlate the check, for example).	1				
22	It should be possible to acquire privacy-enhancing single-use credentials from a long-lived credential.					
23	It should be possible to blind-sign portions of the credential data (such as a unique credential identifier) for certain use cases so that issuers cannot track usage even when inspectors collide with them.					
24	It should be possible to countersign a credential (multi-sig support) and a profile of multiple credentials.					
25	It should be possible to add additional "endorsement" style signatures to a verifiable claim/credential/profile. It should be possible to "chain" these signatures, where each signature in the chain incorporates all of the previous ones in the chain.					
26	There should be some common vocabulary terms for expressing fundamentals such as the issuer, subject, etc.					
27	There should be a common vocabulary term for expressing alternative identifiers to enable delegation to issuing agents that may generate their own identifiers for					
	credentials (i.e. a piece of software may delegate the issuing of credentials to another agent and it should be possible for the software to express a unique identifier for that credential that is in a namespace the software manages and that may be a different identifier than the one the agent (or holder) assigns to the credential; note that this is not for privacy-enhanced credential identifier use cases).					
28	It should be possible to counter-sign a credential or profile in a way that limits the usage of that credential or profile in a variety of ways, at a minimum, its usage at a					
29	particular domain. It should be possible for inspectors (or holders) to express how they intend to use credentials or profiles and for holders to counter-sign credentials or profiles with an activate hold resolution of the profiles in the profiles of the profiles and the profiles and for holders to counter-sign credentials or profiles with an					
30	It should be possible to express expiration periods (preferably validity periods i.e. start and expiration times).					
31	It should be possible to use the same data structure via an HTTP message, via a browser communication channel (postMessage, serviceWorker, etc.), and via					
32	Be able to specify nature of attestment (native (i.e. Twitter attests that I'm @ChristopherA which they control) or confirm (Someone other than Twitter validates that I					
22	possess @ChristopherA at a particular time, but they don't control @ChristopherA) Proceed for Association, Evidence and Evaluation as not https://withub.com/MchOFTruttleforatable.com/thice_toolk/it					
34	rioposa no Asseriuon, Ervience and Evaluation as per https://gittub.com/web/ormsum/uppriade=reputation-tookit I should be possible for issuere to inserte their useries policies into issued organization. Evaluation in the inserted and an and a second					
34	te should be possible for issuers to insert their usage policies into issued determals. Policy rules include such timings as valuary times, single/inductive usage, revocation info, inspector white or black lists, and any other rules that are understood by a community of credential stakeholders.					
35	Data objects, elements, and vocabulary terms in the data model should use or reference or align to existing standard vocabularies rather than create new definitions for common terms (e.g. Schema.org, CEDS, DCMI).					
36	Data objects, elements, and vocabulary terms should link to human-readable definitions, not just technical definitions with an assumed context, so non-technical audiences can understand what the data means.					
37	Any verifiable claim that represents a credential earned by a person or organization demonstrating competencies or performance tasks should link to standard definitions of those competencies using a structure like schema.org AlignmentObject https://schema.org/AlignmentObject. The target of each alignment may be machine-readable and human-readable definitions of the competency.					
38	The subject of the claim should be able to have the ability to refute the claim being made about them.					
39	It must be possible to publish a verifiable claim on an HTML Web Page such that a search engine can verify the authenticity of the information and index the information.					
40	It should be easy for a Web Developer to see (via view source or DOM inspection) what verifiable claims their website is publishing.					
41	It must be possible to extend the semantic meaning of verifiable claims without having to coordinate with a central repository.	1				
42	It should be possible to store credentials in a document-style/NoSQL or graph database without harming accessibility to the data or the ability to verify its authorship in a significant way.					
	(Total points should be 10)	10				