	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 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**	0				
ID	**Requirements Ordering**	(Org name)				
1	It must be possible for any entity to issue a verifiable claim. (originally from UCR4.1)					
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)					
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)					
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, 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.					
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 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 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).					
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 significant way.					
	(Total points should be 10)	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 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 R**
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)	7	1	1	1	1	1	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)	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 issuer. (originally from UCR4.3)	5		1	1		1	1	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)	5	1	1	1		1	1	
7	It must be possible to verify claims in an automated fashion. (originally from UCR4.3)	4		1	1			1	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)	4	1	1			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		1		1			1
14	The data model should be signature scheme agnostic (should work with JWT, LDS, etc.)	3	1		1			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).	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 merged 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 than 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 context, so non-technical audiences can understand what the data means.	1				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-readable and human-readable definitions of the competency.	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 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).	0							
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 than 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 information 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 ability 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 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**	10				
ID	**Requirements Ordering**	University of Málaga				
1	It must be possible for any entity to issue a verifiable claim. (originally from UCR4.1)					
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 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.	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 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.	1				
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 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 (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.	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-readable and human-readable definitions of the competency.	1				
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 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**	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 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)					
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)	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)	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).	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 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 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).					
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.	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 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**	10				
ID	**Requirements Ordering**	Accreditrust				
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 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 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 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 (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 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**	10	10	10	10		4
ID	**Requirements Ordering**	**Pearson**	**ETS**	**Digital Bazaar**	**uma.es**	**sum of votes**	**average**
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	1	1	1	4	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	1	1		3	0.75
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	1	1	1	4	1
1	It must be possible for any entity to issue a verifiable claim. (originally from UCR4.1)	1		1		2	0.5
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		1	2	0.5
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)	1	1			2	0.5
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	1	1	3	0.75
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	1			2	0.5
14	The data model should be signature scheme agnostic (should work with JWT, LDS, etc.)	1		1		2	0.5
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				1	0.25
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	1	0.25
30	It should be possible to express expiration periods (preferably validity periods i.e. start and expiration times).	1			1	2	0.5
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		2	0.5
7	It must be possible to verify claims in an automated fashion. (originally from UCR4.3)		1	1		2	0.5
9	It must be possible for the holder to move a claim among credential repositories. (originally from UCR4.4)		1			1	0.25
12	The data model should be identifier agnostic (limiting to URIs is fine).			1		1	0.25
13	The data model should be data syntax agnostic (should work in XML, JSON, CBOR, XDI, etc.)			1		1	0.25
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	1	0.25
19	There should be a standard way to combine multiple sets of claims to produce a profile about a particular subject.					0	0
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	0.25
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	0
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				1	0.25
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.				1	1	0.25
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.				1	1	0.25
41	It must be possible to extend the semantic meaning of verifiable claims without having to coordinate with a central repository.					0	0
16	It must be possible to express data in a way such that term collisions (key-value pairs) are guaranteed to not happen.					0	0
18	It should be possible to have digitally signed data at multiple levels of nesting.					0	0
20	It should be possible to express a revocation list for a particular set of claims.					0	0
22	It should be possible to acquire privacy-enhancing single-use credentials from a long-lived credential.					0	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	0
24	It should be possible to countersign a credential (multi-sig support) and a profile of multiple credentials.					0	0
26	There should be some common vocabulary terms for expressing fundamentals such as the issuer, subject, etc.					0	0
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).					0	0
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	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	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 than Twitter validates that I possess @ChristopherA at a particular time, but they don't control @ChristopherA)					0	0
33	Proposal for Assertion, Evidence and Evaluation as per https://github.com/WebOfTrustInfo/portable-reputation-toolkit					0	0
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.					0	0
38	The subject of the claim should be able to have the ability to refute the claim being made about them.					0	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 information and index the information.					0	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	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 ability to verify its authorship in a significant way.					0	0
	(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 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**	10					
ID	**Requirements Ordering**	ETS					
1	It must be possible for any entity to issue a verifiable claim. (originally from UCR4.1)						
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)	1					
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)	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 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 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 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 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).						
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 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 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**	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)					
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 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 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 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).					
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 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 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**	10				
ID	**Requirements Ordering**	Legendary Requirements (Joe Andrieu)				
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)	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)					
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)					
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)	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)	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 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 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 acknowledgement/acceptance 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.	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				