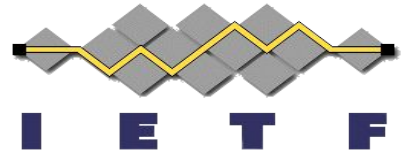
SPICE

`draft-prorock-spice-use-cases`

(or: i am sure there is a reason we started a kerfuffle)

IETF 120, Vancouver

July, 2024



Why are we here? (specifically for SPICE, not existentially)

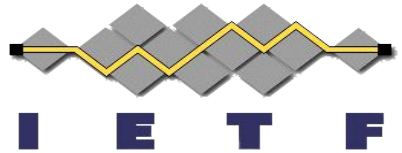
To document and define use of 3 party model credentials with COSE

Especially m2m use cases, not human in the loop

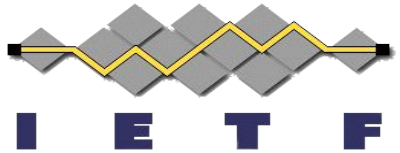
a quick definition set:

- An "issuer", an entity (person, device, organization, or software agent) that constructs and secures digital credentials.
- A "holder", an entity (person, device, organization, or software agent) that controls the disclosure of credentials.
- A "verifier", an entity (person, device, organization, or software agent) that verifies and validates secured digital credentials.

SPICE Use Cases draft-prorock-spice-use-cases-01



- A need for selective disclosure with CBOR based verifiable credentials
- Cryptographic agility support via COSE, including support for PQC, and to permit use of the same signature algorithms with both selective disclosure as well as fully disclosed credentials
- Required strong and long lived identities that are correlated with public key material for verifiacation and permit binding to DNS, existing x509 certificates, as well as providing ready access to public keys for verification utilizing HTTP

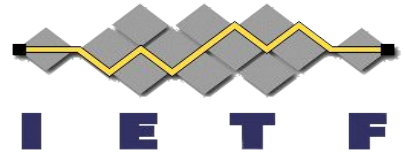


Physical Supply Chain Credentials

- Import permits
- Traceability

Credentials related to Authenticity and Provenance

- Ownership / Provenance of data
- Authenticity of data



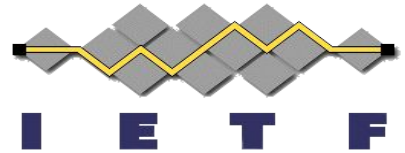
What's next?

SPICE

`draft-steele-spice-profiles-bcp`

(or: how do we help the business side out)

IETF 120, Vancouver
July, 2024



What the heck is this doc and why did you folks put it together?

provide a bridge for policy/regulatory/business to write their requirements in a way that permits translation into appropriate technical specs / schemas

break the need for inline XML (and sometimes JSON or CBOR) out of docs that tell folks what needs to be in a credential

Why did you folks put it together (continued)?

help provide a simpler path to upgraded encoding of data

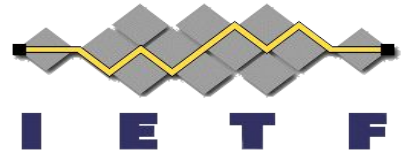
provide standard guidance that helps split the:

- ***Data shape*** *from the*
- ***Data encoding*** *from the*
- ***Securing mechanism*** *from the*
- ***Transport mechanism***

} this draft helps here

Why did you folks put it together (continued)?

because I was asked to help provide guidance for how to bind regulatory data requirements to data formats without linking standard ways of encoding data to dictionaries of data fields controlled by regulatory agencies



An example case

As a policy maker in international trade, I need to be in control of changes to what data fields can be collected, when that data can be collected, and from whom. I might have some basic constraints on that data.

I want to use open standards for data encoding, security, and exchange of that data, but I don't know if we will upgrade our security guidelines or encoding requirements at a later date.

I would like to lay out a table of what the data should look like, and have a corresponding section that specifies what the allowed security parameters are, so that we can revise the data formats later, or the security and other requirements later, but independently of each other.

SPICE-PROFILES draft-steele-spice-profiles-bcp-01

An example case from a current policy doc's data dictionary

SPS Exchange Document

Document Level (DOC)	PC element	PC Element subdivision	Schema Tag	PC	PC/R	Schema notes	Printable example		Format	Cardinality	
										#PC	# PC/R
Type of Document	Certificate name	Certificate name	SPSExchangedDocument.TypeCode	<ram:TypeCode>**851**</ram:TypeCode>	<ram:TypeCode>**657**</ram:TypeCode>	Document Codes	PHYTOSANITARY CERTIFICATE	PHYTOSANITARY CERTIFICATE FOR RE-EXPORT	Numeric	1..1	
NON PC FIELD			SPSExchangedDocument.Name	<ram:Name/>		Name is NOT a Phytosanitary Certificate field and it is present only to comply with the UN/CEFACT schema.				1..1	
Certificate Number	No.	No.	SPSExchangedDocument.ID	<ram:ID>**123ABC**</ram:ID>		Countries may use the same numbering technique. Countries need to use number + country, to identify the correct certificate.	**123ABC**		Text (60)	1..1	
Issuing NPPO	Plant Protection Organization of	name of the NPPO	SPSExchangedDocument.IssuerSPSParty.Name	<ram:IssuerSPSParty> <ram:Name>**Servicio Nacional de Sanidad y Calidad Agroalimentaria**</ram:Name> </ram:IssuerSPSParty>		Name of the issuing NPPO	Servicio Nacional de Sanidad y Calidad Agroalimentaria		Text (256)	1..1	
Status and date of status change	Name of authorized officer, date and signature	Date of issuance	SPSExchangedDocument.StatusCode	<ram:StatusCode>**70**</ram:StatusCode>		Status Codes	Countries should consider displaying the certificate status in their system.		Numeric	1..1	
			SPSExchangedDocument.IssueDateTime.DateTimeString	<ram:IssueDateTime> <udt:DateTimeString>**2016-04-22T13:53:08-03:00**</udt:DateTimeString> </ram:IssueDateTime>		Date of status change. (i.e. if the certificate is withdrawn, the date of the withdrawal is used.)	2016-April-22		Date Time W3 Format YYYY-MM-DDThh:mm:ssTZD	1..1	
		Name of authorized officer	SPSExchangedDocument.SignatorySPSAuthentication.ProviderSPSParty.SpecifiedSPSPerson.Name	<ram:SignatorySPSAuthentication> <ram:ProviderSPSParty> <ram:SpecifiedSPSPerson> <ram:Name>**Miguel Perrerra** </ram:Name> </ram:SpecifiedSPSPerson> <ram:Name/> </ram:ProviderSPSParty> <ram:IssueSPSLocation> <ram:Name> **La Plata, Buenos Aires**</ram:Name> </ram:IssueSPSLocation> <ram:ActualDateTime> <udt:DateTimeString/> </ram:ActualDateTime>	<ram:SignatorySPSAuthentication> <ram:ProviderSPSParty> <ram:SpecifiedSPSPerson> <ram:Name>**Miguel Perrerra**</ram:Name> </ram:SpecifiedSPSPerson> <ram:Name/> </ram:ProviderSPSParty> <ram:IssueSPSLocation> <ram:Name> **La Plata, Buenos Aires**</ram:Name> </ram:IssueSPSLocation> <ram:ActualDateTime> <udt:DateTimeString/> </ram:ActualDateTime>	Name of authorized officer. Note that the attribute languageID is not used in the name tag.	17. NAME OF AUTHORIZED OFFICER **Miguel Perrerra**		Text (256)	1..1	
NON PC FIELD			SPSExchangedDocument.SignatorySPSAuthentication.ProviderSPSParty.Name			it is present only to comply with the UN/CEFACT schema				1..1	
Place of issue	Place of issue		SPSExchangedDocument.SignatorySPSAuthentication.IssueSPSLocation.Name			Place of issue. Note that the attribute languageID is not in use in the name tag.	PLACE OF ISSUE **La Plata, Buenos Aires**		Text (256)	1..1	
NON PC FIELD			SPSExchangedDocument.SignatorySPSAuthentication.ActualDateTime			it is present only to comply with the UN/CEFACT schema				1..1	

SPICE-PROFILES draft-steele-spice-profiles-bcp-01

What could go away… (and then permit an upgrade path)

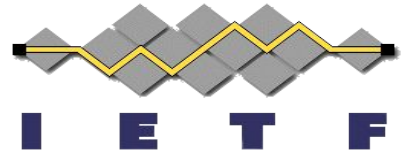
SPS Exchange Document

Document Level (DOC)	PC element	PC Element subdivision	Schema Tag	PC	PC/R	Schema notes	Printable example		Format	Cardinality	
										#PC	# PC/R
Type of Document	Certificate name	Certificate name	SPSExchangedDocument.TypeCode	<ram:TypeCode>**851**</ram:TypeCode>	<ram:TypeCode>**657**</ram:TypeCode>	Document Codes	PHYTOSANITARY CERTIFICATE	PHYTOSANITARY CERTIFICATE FOR RE-EXPORT	Numeric	1..1	
NON PC FIELD			SPSExchangedDocument.Name	<ram:Name/>		Name is NOT a Phytosanitary Certificate field and it is present only to comply with the UN/CEFACT schema.				1..1	
Certificate Number	No.	No.	SPSExchangedDocument.ID	<ram:ID>**123ABC**</ram:ID>		Countries may use the same numbering technique. Countries need to use number + country, to identify the correct certificate.	**123ABC**		Text (60)	1..1	
Issuing NPPO	Plant Protection Organization of	name of the NPPO	SPSExchangedDocument.IssuerSPSParty.Name	<ram:IssuerSPSParty> <ram:Name>**Servicio Nacional de Sanidad y Calidad Agroalimentaria**</ram:Name> </ram:IssuerSPSParty>		Name of the issuing NPPO	Servicio Nacional de Sanidad y Calidad Agroalimentaria		Text (256)	1..1	
Status and date of status change	Name of authorized officer, date and signature	Date of issuance	SPSExchangedDocument.StatusCode	<ram:StatusCode>**70**</ram:StatusCode>		Status Codes	Countries should consider displaying the certificate status in their system.		Numeric	1..1	
			SPSExchangedDocument.IssueDateTime.DateTimeString	<ram:IssueDateTime> <udt:DateTimeString>**2016-04-22T13:53:08-03:00**</udt:DateTimeString> </ram:IssueDateTime>		Date of status change. (i.e. if the certificate is withdrawn, the date of the withdrawal is used.)	2016-April-22		Date Time W3 Format YYYY-MM-DDThh:mm:ssTZD	1..1	
		Name of authorized officer	SPSExchangedDocument.SignatorySPSAuthentication.ProviderSPSParty.SpecifiedSPSPerson.Name	<ram:SignatorySPSAuthentication> <ram:ProviderSPSParty> <ram:SpecifiedSPSPerson> <ram:Name>**Miguel Perrerra** </ram:Name> </ram:SpecifiedSPSPerson>	<ram:SignatorySPSAuthentication> <ram:ProviderSPSParty> <ram:SpecifiedSPSPerson> <ram:Name>**Miguel Perrerra**</ram:Name> </ram:SpecifiedSPSPerson>	Name of authorized officer. Note that the attribute languageID is not used in the name tag.	17. NAME OF AUTHORIZED OFFICER **Miguel Perrerra**		Text (256)	1..1	
NON PC FIELD			SPSExchangedDocument.SignatorySPSAuthentication.ProviderSPSParty.Name	<ram:Name/> </ram:ProviderSPSParty>	<ram:Name/> </ram:ProviderSPSParty>	it is present only to comply with the UN/CEFACT schema				1..1	
Place of issue	Place of issue		SPSExchangedDocument.SignatorySPSAuthentication.IssueSPSLocation.Name	<ram:IssueSPSLocation> <ram:Name>**La Plata, Buenos Aires**</ram:Name> </ram:IssueSPSLocation>	<ram:IssueSPSLocation> <ram:Name>**La Plata, Buenos Aires**</ram:Name> </ram:IssueSPSLocation>	Place of issue. Note that the attribute languageID is not in use in the name tag.	PLACE OF ISSUE **La Plata, Buenos Aires**		Text (256)	1..1	
NON PC FIELD			SPSExchangedDocument.SignatorySPSAuthentication.ActualDateTime	<ram:ActualDateTime> <udt:DateTimeString/> </ram:ActualDateTime>	<ram:ActualDateTime> <udt:DateTimeString/> </ram:ActualDateTime>	it is present only to comply with the UN/CEFACT schema				1..1	

As it stands today the entire document would need to be revised and approved just to add a JSON or CBOR representation of the data.

This ends up locking services that are fully “compliant” with the policy to an extensive XML schema, with no clean upgrade path between international parties.

Ideally the policy docs could describe the data in a clean table that is separated from the xml schema….

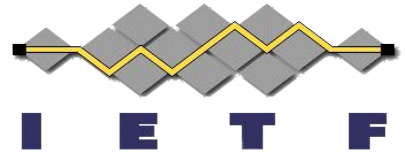


with guidance from this draft, a section of the transformed doc could look (something) like:

Doc Level	Parent	FieldName	Description	Format
Status	SPSExchangedDocument	StatusCode	Status of doc	TinyInt
Status	SPSExchangedDocument	Issued	Issued date	ISODateTime
Status	SPSExchangedDocument	Issuer	Issuer of the doc	String(256)

which could then be used to programmatically generate a JSON Schema, JSON-LD Context, etc. as might be required

Assuming of course a separate section on approved encodings



Questions for the group

Any questions for me (or other authors/contributors)?

Adoption?