



# Technical report

## Privacy Protocol semantic criteria list and privacy-preserving credentials format

backward ref. : TR-Privacy\_Preserving\_Credentials\_MFaher-02-11-2010\_v10.pdf  
and privacy-semantic-rev3\_05112010\_MFaher.doc

## ***table of contents***

table of contents.....	2
Document History .....	3
Scope .....	4
Glossary .....	4
Criteria list format.....	5
Coding example .....	8
Criteria list footprint .....	9
Identification attributes versus privacy.....	10
Criteria list processing by Identity Provider.....	14
Privacy-preserving credentials format .....	14
Coding example .....	15
Privacy-preserving credentials loading .....	16

## Document History

Contributors	Date	Main Changes	Comments
M.Faher-Gemalto	Nov 2nd 2010	Rev1	Proposal for implementation of the privacy protocol, DO & files structure, COMPARE cmd param.
Mourad Faher –Gemalto STD , J.-P.T & O.Joffray- Gemalto R&D	Nov 2nd 2010	Rev2	Review and shortlist of privacy attributes/files
M.Faher & Y.Varuhaki - Gemalto	Nov 3rd 2010	Rev.2	overall review of privacy attributes with MKT from use case standpoint
M.Faher-Gemalto & A. Feraud - Oberthur	Nov 4th 2010	Rev3 : restrictions on CQ for COMPARE cmd, extension of CVD, agreement on dedicated privacy features/files, clearing ambiguity for age verification	Review with Oberthur for agreement : Minutes of sessions issued.
M.Faher-Gemalto & A. Feraud – Oberthur	Nov 5th 2010	Rev3 : consolidation	Review for consolidation of agreed changes in the draft
M.Faher-Gemalto	Nov 19th 2010	Rev4	Addition of the privacy-preserving credentials format and coding. Replacement of DO'53' with DO'73' (acc. ISO/GE4 resolution for comments on CD2 7816-4), assignment of DO Tag for criteria list on Table 6.
A.Feraud-Oberthur & M.Faher-Gemalto	Nov 26th	Rev5	Review and Enhancement of the CVD with new modes and completion of credentials format. + Ed. corrections on Table 5 & 8
M.Faher	Dec 20 <sup>th</sup>	V1.5	Ed. Update : doc title, p.1 Headers& Footers, scope, table-2 footnote w. mention of DOs storing id. attributes
M.Faher acc. Gemalto team	April 20 <sup>th</sup> 2011 April 30 <sup>th</sup> 2011 May 10 <sup>th</sup> 2011 Aug 10 <sup>th</sup> 2011 Aug 17 <sup>th</sup> 2011	V1.6 V1.7 V1.7 V2.0 V2.1	Introduction and enforcement of a CR M/O attribute for each criterion in Criteria List, expiration date handling, Edit. updates

## **Scope**

This document completes and amends the TR bearing on *Privacy-Preserving-Credentials*

This document is a proposal for interoperable encoding of the criteria list issued by Service Providers for the purposes of the mERA-based Privacy Protocol; additionally, this document describes the privacy-preserving credentials format as it shall be generated by the Identity Provider.

## **Glossary**

criteria list	set of queries delivered by the SP and respective to a e-Service
privacy-preserved credentials	IdP-validated list of criteria including card ephemeral public key
administrative files	files hosting user's identification data as determined by the issuing National instance and not involved in the privacy scheme herein specified
privacy-enabling eServices files	set of files dedicated to eServices access with privacy
identification attributes	restricted set of Data Elements or bytestrings or Data Objects contributing to user identification for access to eServices with privacy and that are structured in dedicated files.
privacy features	other wording for identification attributes

## Criteria list format

The criteria list delivered by the Service Provider shall conform to the following structure:

**Table 1 —Profile structure (criteria list for mERA)**

Tag	Length (byte)	Value /Meaning			M/O
'73'	var	Discretionary template containing context-specific DOs for comparison data with value interpreted as binary coded numbers			M
		Tag	Length	Value/Meaning	
		'81'	1 or 2	CVD (Criteria validity duration ref. Table 4)	M
		'18'	var	CVD Expiration date (acc. ISO 8601)	O
		'80'	1	CR (Criterion Requirement according Table 3) employed to denote the whether a criterion is mandated or not. One-byte length DO.	M
		'XY'	var	CQ (note 1) Comparison data bearing on either an EF or a DO hosting user identification attribute, with X from '8' to 'B' and Y from '7' to 'F' (note 2)	M

Note 1: CQ (Comparison Qualifier) is according Table 2

Note 2: the list of DOs for comparison is to be completed according Table 8— list of optional identification attributes and applicable rules.

The context-specific DOs for comparison comprise the criteria list of the required profile for accessing a eService along with its respective validity period (CVD) applying to the whole criteria list. These DOs may be expanded provided they bear upon files (EF) or containers (DO) with interoperable identifiers defined in Cryptographic Information Application (ISO 7816-15)

Only non"RFU" options in Table 2 are applicable in the present specification.

**Table 2— Comparison Qualifier (CQ)**

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	-	x	x	<b>COMPARE command function (P1 value)</b>
-	-	-	-	-	-	0	0	- COMPARE BINARY
-	-	-	-	-	-	0	1	- COMPARE RECORD (RFU)
-	-	-	-	-	-	1	1	- COMPARE DATA (note 2)
-	-	-	x	x	x	-	-	<b>Comparison qualifier (COMPARE P2 value)</b>
-	-	-	0	0	0	-	-	- comparison defined by an OID DO'06' (RFU)
-	-	-	0	0	1	-	-	- values shall be equal
-	-	-	0	1	0	-	-	- reference data shall be higher than target DO value
-	-	-	0	1	1	-	-	- Reference data value shall be smaller than target DO value
-	-	-	1	0	0	-	-	- Reference string value shall be different from target DO value
-	-	-	1	0	1	-	-	- Reference value shall be within the inclusive value range (note 1)
-	-	-	1	1	0	-	-	- Reference value shall not be within the inclusive value range (note 1)
Any other value is RFU								Note 1: For b5-b3='101'b or '110'b, further Data elements representing the inclusive value range encapsulated in DO'80' shall be nested in the subsequent bytes Note 2: this P1 option may be used when user identification attributes are stored in DOs

**Table 3 —Mandatory/Optional attribute or Criterion Requirement (CR)**

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	-	x	x	<b>Criterion attribute (M/O)</b>
-	-	-	-	-	-	0	0	Optional criterion (not mandated by the SP)
-	-	-	-	-	-	0	1	Mandatory criterion (mandated by the SP)
Any other value is RFU								

The Criterion Requirement (CR) shall be used for user's convenience : the user may deselect during the transaction with IdP an optional criterion that he formerly ticked off with the SP. The mandatory criteria are not assumed to be deselected by the user otherwise the service couldn't be accessible unless determined otherwise by the SP.

The CR is encapsulated in DO'80' and applies only to the succeeding criterion. In discretionary template DO'73' many occurrences of DO'80' may be present, each of which relates to the just succeeding criterion.

Any criterion in the Criteria List shall be assigned a CR DO'80'. in case the CR is not present with a criterion in the Criteria List, the default CR value for this criterion shall be CR = 0x01.

**Table 4 — Criteria validity duration (CVD)**

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	<b>Validated criteria to be used once</b> (i.e valid for a unique access)
1	1	1	1	1	1	1	1	<b>Validated criteria with no time limit</b> (i.e valid over card lifespan)
X	X	X						<b>Duration unit</b>
0	0	0	-	-	-	-	-	Duration unit = day
0	0	1	-	-	-	-	-	Duration unit = month
0	1	1	-	-	-	-	-	Duration unit = usage allowance (number of authorized use)
1	0	1	-	-	-	-	-	Duration unit = usage allowance x 10 (tens of authorized use)
0	1	0	-	-	-	-	-	Duration unit = usage allowance (number of authorized use) within a given validity period
1	0	0	-	-	-	-	-	Duration unit = usage allowance x 10 (tens of authorized use) within a given validity period
-	-	-	X	X	X	X	X	<b>Duration value</b> (from 1 to 31 duration unit) In case of a mixed duration unit combining validity period and number of authorized use i.e.bits 8 to 6 equal to '010' or '100' , bits 5 to 1 encode the usage allowance and a further byte (Table 5 —CVD extension) encodes the validity period.
Any other value is RFU								when CVD is absent from the context-specific DO for comparison, the default value is '00' (unique access)

In case the duration unit combines both a usage allowance and a validity period, the CVD shall be completed with a second byte used to encode the validity period

**Table 5 —CVD extension**

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	x	x	x	x	x	x	x	<b>Validity period (in days)</b>
1	x	x	x	x	x	x	x	<b>Validity period (in months)</b>

By definition, the start date for the credentials corresponds to the date or very moment when the user presents these credentials to the SP in view of accessing a service. Accordingly, if an expiration date is present in the criteria list / credentials, the criteria validity duration (CVD) takes effect from this moment onward up to the expiration date.

The expiration date, if present, shall be encoded as a DO with a tag of [UNIVERSAL 24] class (ASN.1 encoding rules, ISO/IEC 8825-1) and nested within the criteria list. The following rules apply :

- i. the value of type GeneralizedTime is a character string of type VisibleString with lexical restrictions as : a string of the form "YYYYMMDDhh[mm[ss[(.)ffff]]]" standing for a local time, with four digits for the year (YYYY), two for the month (MM), two for the day (DD) and two for the hour (hh), followed by two digits for the minutes (mm) and two for the seconds (ss) if required, then a dot or a comma, and a number indicating the fractions of second, the maximum precision depending on the application (ref. ISO 8601), e.g. : if the expiration date is August 10<sup>th</sup> 2011 at 7:30PM, the value field of GeneralizedTime DO is "201108101930"
- ii. a string conforming to the description above (i) and followed by the lettre "Z" would denote a UTC time (Greenwich meridian time or Greenwich Main Time), e.g. : if expiration date according Greenwich Main Time is 8AM on August 10<sup>th</sup> 2011, the value field of GeneralizedTime DO is "201108100800Z"

- iii. a string conforming to (i) and followed by a string "(+|-)hh[mm]" entails that the GeneralizedTime is the difference between the string of (i) and the second string, whereby giving the time lag if required, e.g. : if expiration date local time is 8AM on August 10<sup>th</sup> 2011 and co-ordinated universal time is 12 noon on August 10<sup>th</sup> 2011, the value field of GeneralizedTime DO is "201108100600-0400"

The following range of values is valid for (i) : YYYY (0000 to 9999), MM (01 to 12), DD (01 to 31), hh (00 to 23), mm (00 to 59), ss (00 to 59).

The string value "YYYYMMDDhh[mm[ss[(.)ffff]]]" shall be encoded as ASCII to Hex then encapsulated in DO '18' for GeneralizedTime.

For the present specification, (i) is the supported option.

## Coding example

The Service Provider may build a criteria list as follows :

```
'73'-L73-{ {'81'-01'-23'} -- "CVD : the criteria herein, once validated by IdP, will grant access to the serviceduring 3 months"  
  {'18'-0C'-32'-30'-31'-31'-30'-38'-31'-30'-30'-38'-30'-30'} -- "the expiration date for the CVD above is August 10th 2011 at 8:00AM"  
  {'80'-01'-01'} -- "fulfilment of the following criterion in the list is mandatory to access the service"  
  {'87'-0A'-14'-19'-87'-01'-01'-FF'-19'-92'-01'-01'} -- "is the card bearer between 18-year old and 23-year old ? reference values are within inclusive range and the COMPARE command function shall be COMPARE BINARY".  
}
```

A separator 'FF' is used between the inclusive limits of a range within which one element matches as per ISO 7816-4 clause 11.4.9.

Inclusive limits of the range are coded with the lowest numerical value first (leftmost bytes, e.g '19'-87'-01'-01') and the highest value afterwards (rightmost bytes e.g '19'-92'-01'-01' ). In this example, the Comparison Qualifier (CQ) evaluates to 0x14 (see its meaning in Table-2)

For age verification, the BCD coding of the inclusive limits of the range is employed to allow for a fast translation of the criteria into COMPARE command parameters by IdP, and to alleviate on-card processing during the comparison.

If IdP notices any inconsistency between Expiration date and current time, he may raise a MISFIT flag through the COMPARE Query Result (QR).

As an example for a service restricted to users between 14-year and 18-year old and for which the requested access validity duration is over one year, the SP may question the cardholder's birth date with the criterion (Tag '87') as : "is the birth date of the cardholder less than (Dcur - 17 years) and greater than (Dcur - 14 years)" and in correlation with this criterion, the SP may fix the expiration date to (Dcur + 1 year) with Dcur being the date of the day when the user loads his criteria list. By doing so, the SP may ensure that in case the user is 17-year old at the current date he could access legally the requested service during one year without infringing the age restriction rules. This is to minimize the risk of having an authorization granted whereas its age criterion is not anymore valid. A certain flexibility may be allowed by the SP depending on his general policy and on the nature of the service. The maximum control on such criterion may be obtained by granting access only once to the age-restricted services but this would hinder the transaction.

The Identity Provider shall built the respective COMPARE command as follows :

**Table 6 —example of COMPARE command and response**

CLA	As defined in ISO 7816-4
INS	'33'
P1	'00' COMPARE BINARY
P2	Operation qualifier : '05' Reference value shall be within the inclusive value range
L <sub>c</sub> field	Present (N <sub>c</sub> > 0)
Data field	DO'60' (as defined in ISO 7816-4 Table 75) : '60'-L <sub>60</sub> { General reference template {4F-L <sub>4F</sub> -AID} card-application hosting the EF.Birth file {51-L <sub>51</sub> -FID} Path to EF.birth (e.g 3F00/FID) {73-'0C'-{'80-'04-'19-'87-'01-'01-'80-'04-'19-'92-'01-'01'}} comparison data encapsulated under '73' }
L <sub>e</sub> field	Absent (N <sub>e</sub> = 0)
Data field	Absent
SW1-SW2	Acc. ISO 7816-4, e.g. '9000', '6282', '6982', '6340'

As per ISO 7816-4 recommendation for response data field when present, the concatenation of two DOs'80' defines the inclusive limits of a range within which one element matches. This alternative was validated with AFNOR ISO/GE4 and will be proposed as official comment to ISO/WG4 on CD2 7816-4.

### **Criteria list footprint**

The criteria list that formatted is supplied to the card by the SP via an EXTERNAL AUTHENTICATE command according mERA mechanism (see Table 7)

**Table 7— EXTERNAL AUTHENTICATE command (ref. mERA stage 5)**

Command parameter	Meaning
CLA	Acc. ISO 7816-4
INS	'82' EXTERNAL AUTHENTICATE
P1 P2	'00' no specific information '00' no key reference
Lc Field	'xx'
Data Field	ENC[K <sup>a</sup> <sub>ENC</sub> ](RND.ICC   Application-specific payload)    MAC[K <sub>MAC</sub> ](ENC[K <sup>a</sup> <sub>ENC</sub> ](RND.ICC   Application-specific payload))

Application-specific payload represents here the entire criteria list (no command chaining required); the maximum length of the Criteria List is thus 207 bytes.

## Identification attributes versus privacy

There are two points of view : either execution of COMPARE command is forbidden at some identification data that could disclose the user's private information (Name, Photo) and allow for tracking, or all identification attributes support the COMPARE command provided user consent and Mutual Authentication are performed properly. With this respect, from Marketing standpoint, user decision should account and the decision as to whether some identification data may be disclosed to a Service Provider should depend on user's willing. This nevertheless may raise the problem of user's maturity : kids or youngsters may need enforcement of their identification data protection. A straightforward solution is to separate between administrative files and privacy-enabling eServices files. Accordingly, only privacy attributes eligible for privacy-enabled access to eServices are listed here below.

Some administrative files may be replicated if needed. Both administrative and privacy-enabling eServices files SHALL be referred to within on-card CIA application (ISO 7816-15 ref. ECC-2)

Administrative and privacy-enabling eServices files MAY be assigned respectively access rules as follows :

Files (EF)	Supported command	Access Rules
Administrative files	SELECT, READ BINARY, GET (NEXT) DATA, PUT (NEXT) DATA, UPDATE BINARY	UP TO ISSUER
privacy-enabling eServices files	SELECT	ALWAYS
	COMPARE BINARY, COMPARE DATA, COMPARE RECORD	Mutual Authentication (e.g. Device authentication with secure messaging with integrity and confidentiality)
	READ BINARY, GET (NEXT) DATA, PUT (NEXT) DATA, UPDATE BINARY	UP TO ISSUER

The liability of the privacy protocol should only bear upon the privacy-enabling eServices files contents contingent on user consent and terminal authentication.

The card-application MAY denote privacy-enabling eServices files by an additional discretionary DO'A5' or DO'85' within the File Control Parameter. Such files MAY support only COMPARE command (and reject READ command).

The card-application MAY distinguish the Access Mode for READ from the Access Mode for COMPARE on the same file by providing two Access Rules (with OR logical combination) the first of which being for READ and the second for COMPARE.

Alternatively, a comment is being addressed to ISO/WG4 for improvement of Access Mode byte granularity for compact format (CD2 7816-4 clause 9.3.2)

**NOTE:** The user is always likely to disclose identification data through GUI forms in web services transactions whereas the same identification data are secured in privacy-enabling eServices files on his card.

The set of identification attributes that may be subject to comparison process (i.e with COMPARE command) is as follows:

alternatively these attributes may be hosted in Data Objects according ISO/IEC 7816-4.

**Table 8— list of optional identification attributes and applicable rules**

Ident. attribute	Details	File (EF)	structure	File Access rules (for COMPARE cmd)	DO Tag	Comparison Qualifier (P1-P2)
Pseudo-Name	May be e.g artistic name or name for access to some eService	EF.Name_pi  With i from 1 to n (n max = 4)  The card MAY support several pseudonyms each of which shall be referenced in CIA application (acc. ECC-2) for interoperability	UTF8String or ASCII char. ext. ISO8859  May equal the user actual name. Up to the cardholder	Mutual Auth	'82' to '85'	P1:'00' P2: =
User name	The actual user name may jeopardize his/her privacy if disclosed.	EF.Name_p0	Family name, given name. UTF8String or ASCII char. ext. ISO8859	Mutual Auth note : risk of jeopardizing privacy if disclosed	'86'	P1:'00' P2: =
Birth date		EF.Birth_p	YYYYMMDD BCD encoding	Mutual Auth.	'87'	P1: '00' P2: [ ], >, <, =
Addr1 (note1)	Zip/postal code	EF.Addr1_p2	ZIP+4: DDDDDDddd  BCD encoding	Mutual Auth.	'88'	P1:'00' P2: =, >, <, [ ]
	State/region/com mune	EF.Addr1_p3	UTF8String or ASCII char. ISO8859	Mutual Auth.	'89'	P1:'00' P2: =
	country	EF.Addr1_p4	ISO 3166-1 numerical : three-	Mutual	'90'	P1:'00'

Ident. attribute	Details	File (EF)	structure	File Access rules (for COMPARE cmd)	DO Tag	Comparison Qualifier (P1-P2)
			digit numeric e.g France = 250  BCD coding	Auth.		P2: =
Addr2	Same as Addr1  Describes user's secondary address	EF.Addr2_px	Same as Addr1	Same as Addr1	'91' to '93'	Same as Addr1
e-Mail	Personal e-Mail address	EF.Mail_p	RFC821(SMTP) ASCII char.	Mutual Auth.	'94'	P1:'00' P2: =
Card Expiry date	Card validity limit date	EF.Exp	YYYYMM BCD encoding	Mutual Auth	'95'	P1: '00' P2: [ ], >, <, =
Card activation date	Date from which the card becomes operational	EF.CED	YYYYMM BCD encoding	Mutual Auth	'96'	P1: '00' P2: [ ], >, <, =
App activation date	On multi-Applicative cards, date from which the card-application becomes operational	EF.AED	YYYYMM BCD encoding	Mutual Auth	'97'	P1: '00' P2: [ ], >, <, =
Cardholder Nationality	Nationality of the cardholder	EF.NAT	ISO 3166-1 numerical : three-digit numeric e.g France = 250  Can be BCD coded	Mutual Auth	'98'	P1:'00'  P2: =
Cardholder sex	Either Male(1), Female(2), notKnown (0), or notApplicable(9)	EF.SX	one-digit coding according ISO 21549-5:2008, BCD coding as: Male(0001), Female(0010), notKnown (0000), notApplicable(1001)	Mutual Auth	'99'	P1:'00'  P2: =
Extra-	Container of a predefined set of	EF.XTR	Coding still to be determined. SP	Mutual	'9A'	P1:'00'

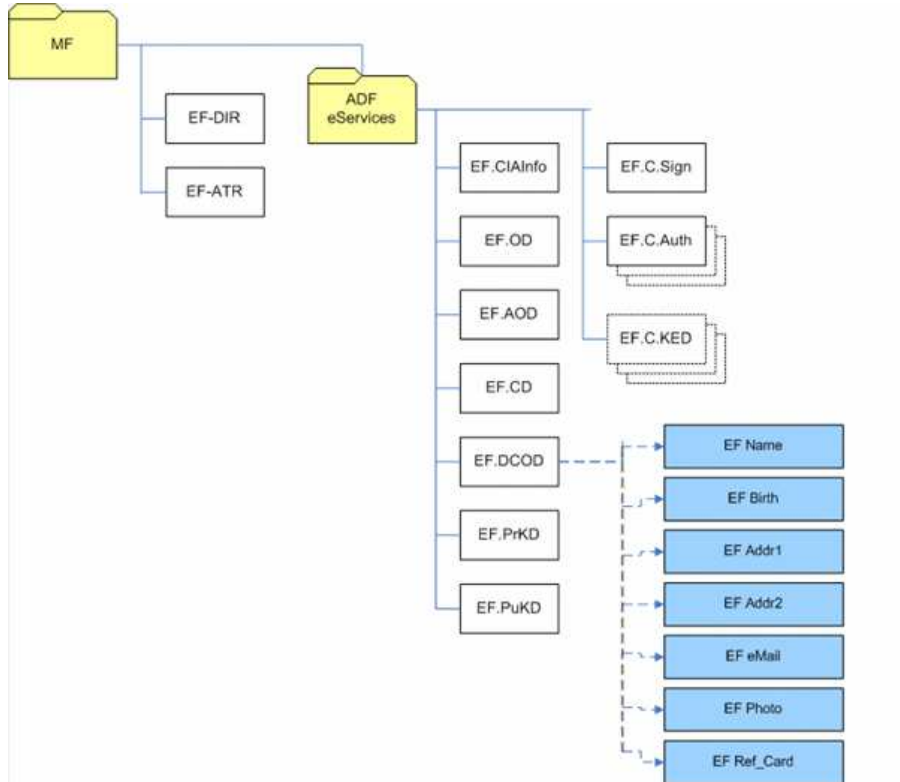
Ident. attribute	Details	File (EF)	structure	File Access rules (for COMPARE cmd)	DO Tag	Comparison Qualifier (P1-P2)
attributes	identification attributes that are personalized upon cardholder request  May contain : Cardholder privilege (e.g VIP club partnership)		may ask the question about a specific Extra-attribute in the list.  ASCII coded	Auth		P2: =

**Note 1:** user address should not contain street name and number otherwise this information would jeopardize privacy. Whenever needed (e.g for supply of goods bought on Internet) the user may type his delivery and invoicing address through a GUI form or the transaction may be held with a trusted intermediary. The infrastructure can be adapted to fulfill the requirements for a payment transaction whereas preserving privacy (not described in the present document).

Figure 1 below show the file system adopted so far for the eService Application Profile / ECC-2.

This set of identification files needs to be extended to enhance privacy design.

**Figure 1 — example of ECC Card File System (eService App Profile)**



## Criteria list processing by Identity Provider

upon recovery of the criteria list, the Identity Provider shall perform the following actions:

- parsing the **EF.DCOD** container within CIA application and matching the identification files available on-card with the attributes that the criteria list bears upon.
- for each **context-specific DO for comparison** in the criteria list : building a COMPARE command with the control parameters denoted in the Comparison Qualifier byte (most significant byte) and a Data field ending with comparison data encapsulated in DO'53' or DO'73' according context-specific DO for comparison's value field.
- sending that constructed COMPARE command to the card.
- recording card's Response APDU as part of the credentials.

## Privacy-preserving credentials format

Once the criteria list is checked by the Identity Provider, this party shall format and incorporate the queries result in a Digital Signature input for validation. According EN14890-1, DSI formats of the digital signature are described for different signature algorithms. It is mandatory to support at least one of these formats. Optionally the card may be able to support other signature formats. The given DSI formats describe the string, that is used directly by the signature algorithm to compute the digital signature.

The Query result from the COMPARE command shall be built by IdP as described in Table 9.

**Table 9 — COMPARE Query Result (QR)**

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	X	X	X	COMPARE query acknowledgement
-	-	-	-	-	0	0	0	YES (COMPARE response with SW1-SW2 = '90 00' with optional Response data Field)
-	-	-	-	-	0	0	1	NO (COMPARE response with i.e SW1-SW2 = '6200')
-	-	-	-	-	0	1	0	NO USER CONSENT (query rejected by the user)
-	-	-	-	-	0	1	1	MISFIT with CVD (e.g. time range of query not compatible with expiration date)
-	-	-	-	-	1	0	0	REFERENCE DATA NOT AVAILABLE (e.g. identification data missing on the card, SW1-SW2='6984')
-	-	-	-	-	1	0	1	QUERY NOT ALLOWED (COMPARE response e.g. with SW1-SW2='6986' or any other similar reason)
Any other value is RFU								

The Query Result (QR) shall be attached to its respective criteria then encapsulated in DO'73' as follows :

'73'-L<sub>73</sub>-{{'81'-'01'-CVD} {'18'-L<sub>18</sub>-ExpDate}{'XY'-L<sub>XY</sub>-comparison data} {'XY'-'01'-QR}} with X from '8' to 'B' and Y from '1' to 'F', and with ExpDate the expiration date if present.

**NOTE** : if used, the DO'80' denoting the "Profile discretionary identifier referencing user's resources hosted by the Service Provider" shall not be part of the criteria list accessible to the Identity Provider. If employed otherwise (i.e to denote whether the criterion is mandated or not) the DO'80' shall be present in criteria list exposed to the Identity Provider.

The card ephemeral public key (PuK.KA.ICC) shall be concatenated to the TLV that obtained and the resulting value shall be hashed (i.e SHA 256) and signed by the IdP (see example below)

## Coding example

On the ground of the COMPARE command example provided in Table 6, the coding of the privacy-preserving credentials is as follows :

```
'73'-L73{ { '42'-'08'-CAR} -- IdP's Certification Authority Reference
            { '06'-Var-OID} -- Digital signature algorithm OBJECT IDENTIFIER (Optional)
            { '81'-'01'-'23'} -- CVD value for 3 months
            { '18'-L18-ExpDate} -- Expiration Date
            { '80'-'01'-'01'} -- CR: the following criterion is mandated by the SP
            { '87'-'0A'-'14'-'19'-'87'-'01'-'01'-'FF'-'19'-'92'-'01'-'01'} -- Range for Age Verification
            { '87'-'01'-'00'} -- QR for "criterion verified"
            { '83'-L83-H(PuK.KA.ICC)} -- hash of card ephemeral public key for Key Agreement
            { '9E'-L9E- IdP signature cryptogram}
        }
```

NOTE : DO'83' MAY be replicated within DO'73': e.g the first occurrence DO being for a comparison data bearing on a pseudonym and the second occurrence for card ephemeral public key for KA.

The IdP applies his signature on the DO'73' as part of the DSI (Digital Signature Input format).

The digital signature input (DSI) processing can be found in EN14890-1 clause 13.3.2 (e.g. for PKCS#1 V1.5 scheme with 2048-bit modulus). The signature from the IdP is executed over the result from COMPARE commands and h(PUK.KA.ICC) which is formatted as follows :

**Table 10— Message (DO'73') to be signed by IdP**

Tag	L			
'73'	L <sub>73</sub>			
		Tag	Length	Value
		'42'	'08'	CAR (Certification Authority Reference)
		'81'	L <sub>81</sub>	CVD (Credentials Validity Duration)
		'18'	L <sub>18</sub>	ExpDate (Expiration date)
		'80'	'01'	Criterion Requirement Mandatory/Optional
		T <sub>Crit.</sub>	L <sub>TC</sub>	Comparison Data
		T <sub>Crit.</sub>	01	Query Result (Verified/Non verified)
		...	....	.....
		'80'	'01'	Criterion Requirement Mandatory/Optional
		T <sub>Crit.</sub>	L <sub>TC</sub>	Comparison Data
		T <sub>Crit.</sub>	01	Query Result (Criterion Verified/Non verified)
		'83'	L <sub>83</sub>	H(Puk.KA.ICC)

Then the DO'73' that constructed is hashed and the hash is submitted to the signature scheme padding then to digital signature.

Once the digital signature is performed the signature cryptogram is nested within a DO'9E' denoting signature and the entire DO'73' is rebuilt. The so completed DO'73' is delivered by IdP to the card. Since the payload size exceeds 255 bytes IdP may have to rely on command chaining.

### ***Privacy-preserving credentials loading***

Once computed, the privacy-preserving credentials are loaded securely onto the card (i.e with PUT DATA command)