CAPE
Card Payments
Terminal Management
Message Usage Guide

Annex B : Key Downloading

Version 6.0

1st December 2017

TABLE OF CONTENTS

1 Download of Cryptographic Keys 4

1.1 Introduction 4

1.2 Notations and Hypothesis 5

1.2.1 Notations 5

1.2.1.1 Hypothesis 6

1.3 Standard Key Download 7

1.3.1 High Level Process 7

1.3.2 Key Status 9

1.3.3 Management Plan with Key Download Action 10

1.3.4 Status Report to Request Key Downloading 11

1.3.5 Configuration Update to Inject Keys 12

1.3.6 Key Download Result 13

1.4 Example 14

1.4.1 Introduction 14

1.4.2 RSA Keys and Certificate 14

1.4.3 Initial Status of the Keys 27

1.4.4 Management Plan with Key Download Action 37

1.4.5 Status Report to Request a Key Download 47

1.4.6 Configuration Update to Inject Keys 60

1.4.7 Key Download Result 69

Figures

Figure 1: Key Information 4
Figure 2: Sharing of a Key with a Host 5
Figure 3: Key and Certificate Notations 5
Figure 4: Encryption and Digital Signature Notations 6
Figure 5: Key Check Value Notation 6
Figure 6: POI and TM PKIs 7
Figure 7: Standard Key Dowload 7
Figure 8: PKI used by the Key Download Example 14

1 Download of Cryptographic Keys

1.1 Introduction

This section specifies the downloading of symmetric cryptographic keys by a Terminal Manager to a POI[1].

These symmetric keys are used:

- Internally by a POI for any kind of protection, or
- To protect data exchanged between the POI and a Host, or between two Hosts.

Protection of the downloaded keys is based on asymmetric cryptographic keys, and may be applied remotely without any particular personalisation of the POI.

These symmetric keys are downloaded through the *AcceptorConfigurationUpdate* message in the *DataSet/Content/SecurityParameters* data structure which contains:

- Some challenges to avoid replay (*POIChallenge*, *TMChallenge*),
- For each symmetric key (*SymmetricKey*):
  - The identification of the key (*Identification*, *AdditionalIdentification*, *Version*),
  - The purpose of the key (*Type*, *Function*),
  - The period of usage (*ActivationDate*, *DeactivationDate*),
  - The value of the key (*KeyValue*).

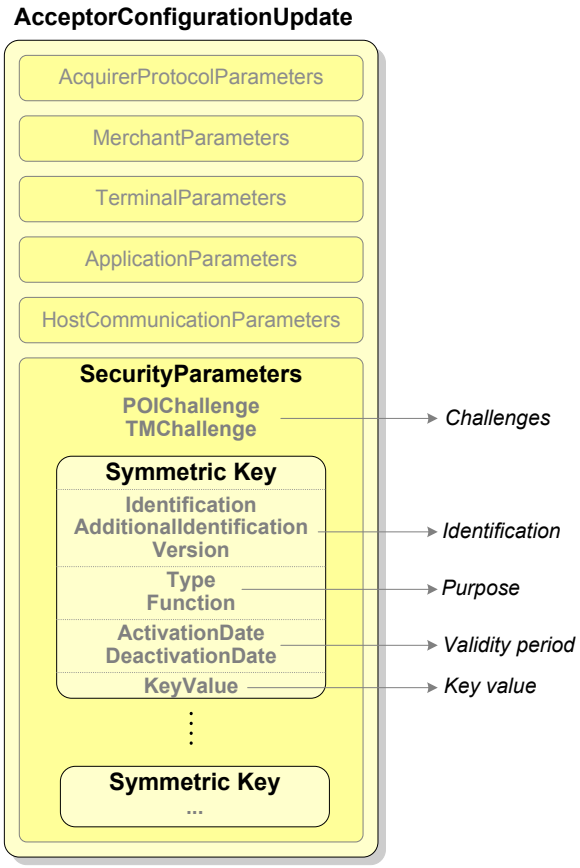

Figure 1: Key Information

[1] The POI should be a POI Terminal, a POI Server, or any Intermediary Agent.

When the symmetric key is shared with a Host, to protect the exchanges with the POI, the configuration of the Host (*HostConfigurationParameters*) contains the identification of the shared keys (*Identification*, *AdditionalIdentification* and *Version*).

It also allows the use of common symmetric key by different hosts.

The configuration of the Host and the configuration of the security are not necessary exchanged in the same *AcceptorConfigurationUpdate* message.

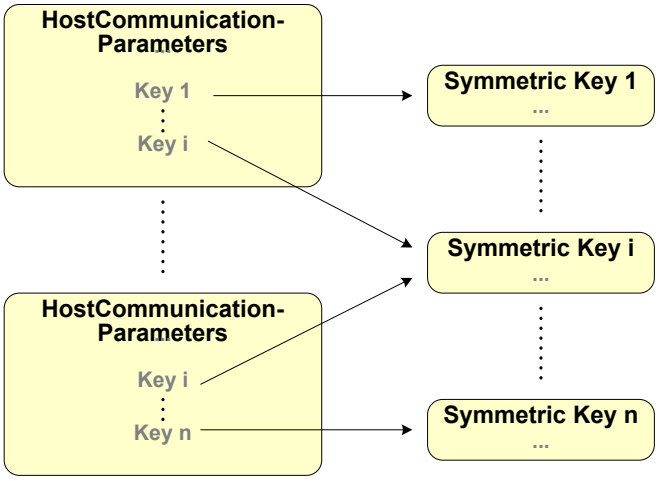

Figure 2: Sharing of a Key with a Host

1.2 Notations and Hypothesis

1.2.1 Notations

Asymmetric keys are denoted $K_{Owner\text{-}Usage}$, where:

- *Owner* of the key is either the POI, denoted *POI*, or the MTM/TM Host, denoted *TM*,
- *Usage* of the key is either the encryption, denoted *Enc*, or the digital signature denoted *Sig*.

X.509 certificates are denoted $Cert_{Issuer\text{-}PKI}(Key)$, where:

- *Issuer* of the certificate is either the Root of the PKI issuing the certificate, denoted *Root* , or the certification authority, denoted *CA*,
- *PKI* is either the POI public key infrastructure, denoted *POI*, or the MTM/TM Host public key infrastructure, denoted *TM*,
- *Key* is the asymmetric key which is certified.

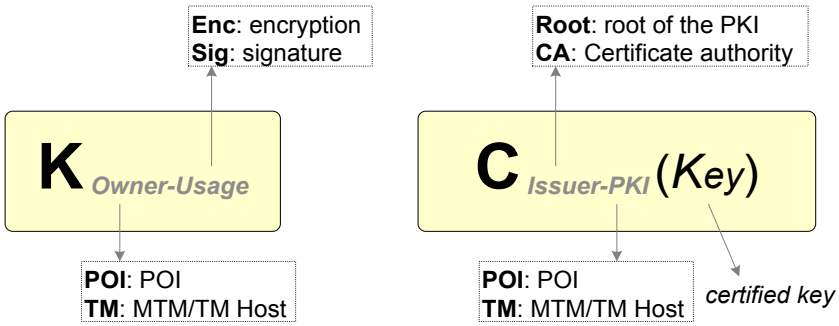

Figure 3: Key and Certificate Notations

Encryptions are denoted *Enc[Key](Data)*, and decryptions *Dec[Key](Data)*, where

- *Key* is the asymmetric key or the symmetric key which has encrypted the *Data*.
- *Data* is the data which is encrypted,

Digital signatures are denoted *Sig[Key](Data)*, where

- *Key* is the asymmetric key which has signed the *Data*.
- *Data* is the data which is signed,

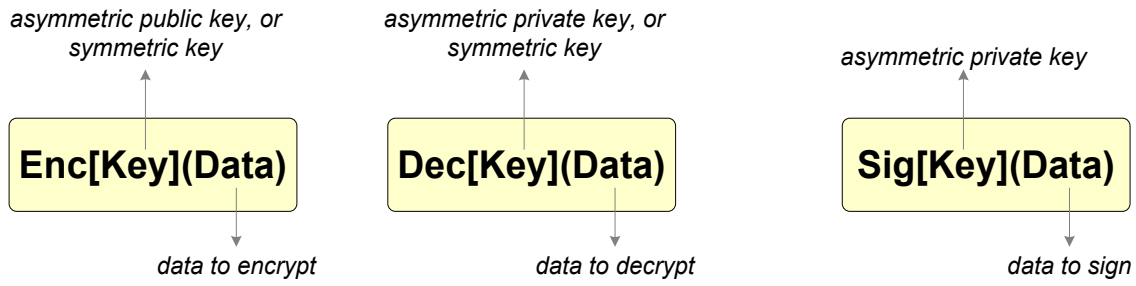

Figure 4: Encryption and Digital Signature Notations

A Key Check Value (KCV) of a symmetric key is denoted *KCV(Key)* and equal to *Enc[Key](00…00)*,

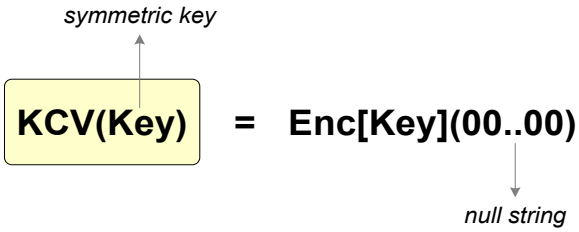

Figure 5: Key Check Value Notation

1.2.1.1 Hypothesis

<u>Hypothesis 1: POI Asymmetric Authentication</u>

The POI owns an authentication asymmetric key $K_{POI\text{-}Sig}$, certified by a certificate authority which has issued the certificate $C_{CA\text{-}POI}(K_{POI\text{-}Sig})$.

The Terminal Manager (TM) has the X.509 certificate $C_{Root\text{-}POI}$ of the root of the POI PKI, or any certificate authority in the chain from the root to the POI authentication asymmetric key $K_{POI\text{-}Sig}$.

<u>Hypothesis 2: TM Asymmetric Authentication</u>

The TM owns:

- An authentication asymmetric key $K_{TM\text{-}Sig}$, certified by a certificate authority which has issued the certificate $C_{CA\text{-}TM}(K_{TM\text{-}Sig})$,
- A key encryption asymmetric key $K_{TM\text{-}Enc}$, certified by the same certificate authority which has issued the certificate $C_{CA\text{-}TM}(K_{TM\text{-}Enc})$,.

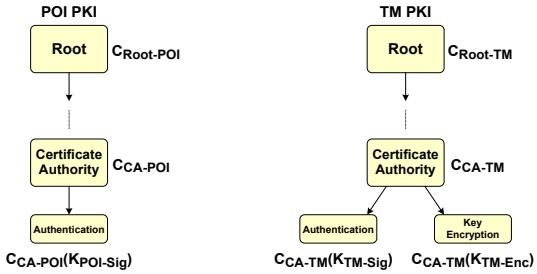

Figure 6: POI and TM PKIs

<u>Hypothesis 3: PKI Organisation</u>

The PKI of the POI and the PKI of the TM may share a common root ($C_{Root-POI} = C_{Root-TM}$).

If the PKI are not shared, the POI has the X.509 certificate $C_{Root-TM}$ of the root of the Terminal Manager PKI, or any certificate authority in the chain from the root to the TM asymmetric keys K_{TM-Sig} and K_{TM-Enc}.

1.3 Standard Key Download

1.3.1 High Level Process

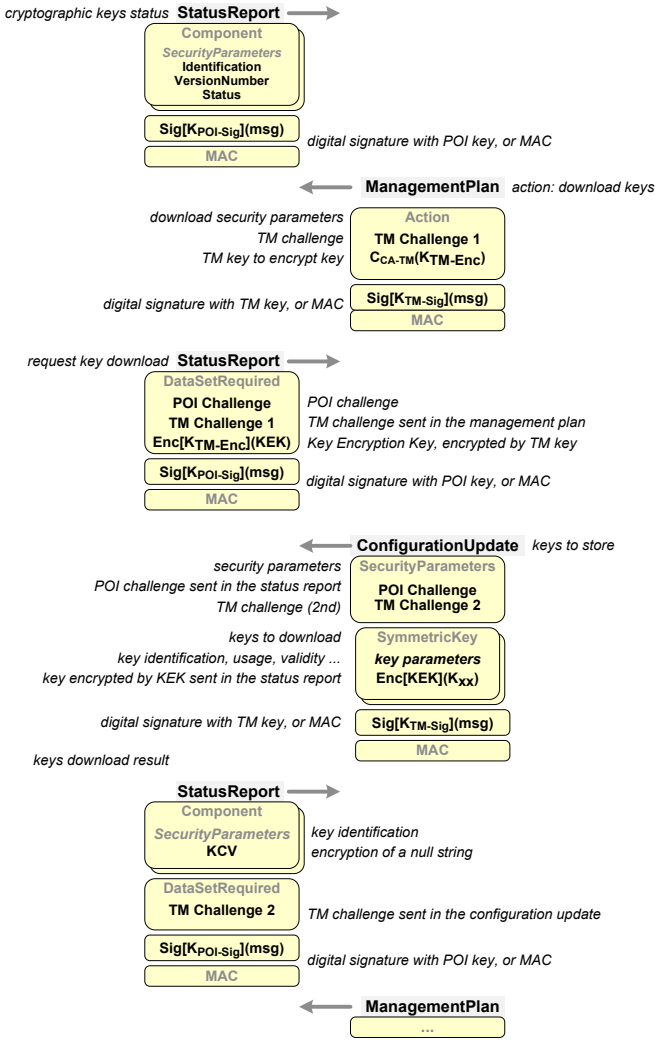

Figure 7: Standard Key Dowload

The standard download of keys performs the following exchanges of messages:

- *Key Status*: The POI sends a *StatusReport* message to the Terminal Manager, in charge of the key download, all the status of the cryptographic keys.
- *Dowload Keys Action*: if some keys or new versions of the keys have to be injected on the POI, the Terminal Manager sends a *ManagementPlanReplacement* message containing an action to download keys (SecurityParameters) with:
  - a first challenge TM Challenge 1 generated by the TM, and
  - the X.509 certificate chain with the $C_{CA\text{-}TM}(K_{TM\text{-}Enc})$ certificate of a public key to encrypt other keys.
- *Request Key Downloading*: following the condition described in the action of the management plan, the POI sends a *StatusReport* message to the Terminal Manager with the *DataSetRequired* containing the identification of the data set with:
  - the challenge TM Challenge 1 sent by the TM,
  - a fresh challenge POI Challenge, generated by the POI,
  - key encryption key KEK, encrypted by the public key $K_{TM\text{-}Enc}$ of the TM: $Enc[K_{TMEnc}](KEK)$

  These data are digitally signed by the POI key $K_{POI\text{-}Sig}$
- *Key Storing*: the TM sends a *AcceptorConfigurationUpdate* message containing:
  - a second fresh challenge TM Challenge 2, generated by the TM,
  - each key to store K_{xx}, encrypted by KEK: $Enc[KEK](K_{xx})$

  These data are digitally signed by the TM private key $K_{TM\text{-}Sig}$
- *Key Dowload Result*: to report the result of the key download action, the POI sends a *StatusReport* message to the Terminal Manager with:
  - the KCV for each loaded key in the related *Component* data structure,
  - the challenge TM Challenge 2 sent by the TM in the *DataSetRequired* data structure,

The Terminal Manager sends a *ManagementPlanReplacement* message containing other actions to perform.

1.3.2 Key Status

Depending on the POI key management, symmetric key may be downloaded periodically by a dedicated action in the management plan, or when required by the TM host depending on the status of the keys loaded on the POI, and provided in the *StatusReport* message.

The status of the keys loaded on the POI is reported in the *Content/Component* of the *StatusReport* with the following structure:

The Multiplicity in the following table should be considered to manage status of keys and not according to the definition of the protocol.

StatusReport/DataSet	*Mult.*	*Usage*
…		
Content	[1..1]	Content of the status report.
…		
POIComponent	[1..*]	Information related to a key loaded in the POI.
Type	[1..1]	“SecurityParameters”
Identification	[1..1]	Identification of the key.
ItemNumber	[0..1]	Identify the hardware or software component loading the key, if defined in another *Component* occurrence.
ProviderIdentification	[0..1]	Identifies the provider or the owner of the key.
Identification	[1..1]	Key indentification.
SerialNumber	[0..1]	see *StatusReport*
Status	[1..1]	Key status.
VersionNumber	[1..1]	Key version.
Status	[1..1]	Current status of the component: *WaitingActivation* The key is not yet valid. *InOperation* The key is activated and in operation. *Deactivated* The key is no more valid or has been deactivated.
ExpiryDate	[0..1]	Expiry date of the Key

This message may be protected in the *SecurityTrailer*:

- by a MAC (*AnthenticatedData*), if the POI own a shared symmetric MAC key, or
- by a digital signature (*SignedData*) of the message, signed by by the POI authentication key $K_{POI\text{-}Sig}$.

1.3.3 Management Plan with Key Download Action

If the key status sent by the POI indicates that some keys or new versions of the keys have to be injected on the POI, the Terminal Manager sends a *ManagementPlanReplacement* message containing an action to download keys with following structure:

The Multiplicity in the following table should be considered to manage key download and not according to the definition of the protocol.

ManagementPlan/DataSet/Content	*Mult.*	*Usage*
Action	[1..1]	Information related to a key download in the POI.
Type	[1..1]	“Download”
RemoteAccess	[0..0]	Not relevant for Key management
TerminalManagerIdentification	[0..0]	Not relevant for Key management
TMSProtocol	[0..0]	Not relevant for Key management
TMSProtocolVersion	[0..0]	Not relevant for Key management
DataSetIdentification	[1..1]	Identification of the set of key to dowload.
Name	[0..1]	Name of the data set.
Type	[1..1]	“SecurityParameters”
Version	[0..1]	Version of the data set.
CreationDateTime	[1..1]	Creation date time of the data set.
ComponentType	[0..*]	“SecurityParameters” may be added
DelegationScopeIdentification	[0..0]	Not relevant for Key management
DelegationScopeDefinition	[0..0]	Not relevant for Key management
DelegationProof	[0..0]	Not relevant for Key management
ProtectedDelegationProof	[0..0]	Not relevant for Key management
Trigger	[1..1]	*see ManagementPlanReplacement*
AdditionalProcess	[0..1]	"Restart": the POI has to restart the application after the successful completion of the action.
Retry	[0..1]	*see ManagementPlanReplacement*
TimeCondition	[0..1]	*see ManagementPlanReplacement*
TMChallenge	[1..1]	Fresh challenge TM Challenge 1 generated by the TM.
KeyEnciphermentCertificate	[1..*]	Certificate chain containing the signed public key encryption key of the Terminal Manager $C_{CA\text{-}TM}(K_{TM\text{-}Enc})$, used by the POI to send a session key encryption key. The certificate chain must ordered by starting with the higher certificate level and ending with the leaf.
ErrorAction	[0..*]	*see ManagementPlanReplacement*

This message may be protected in the *SecurityTrailer*:

- by a MAC (*AnthenticatedData*), if the POI own a shared symmetric MAC key,or
- by a digital signature (*SignedData*) of the message, signed by by the TM authentication key $K_{TM\text{-}Sig}$.

1.3.4 Status Report to Request Key Downloading

According to condition described in the *TimeCondition* of the action sent in the management plan, the POI sends a *StatusReport* message to the Terminal Manager with the following structure:

The Multiplicity in the following table should be considered to manage key download and not according to the definition of the protocol.

StatusReport/DataSet	*Mult.*	*Usage*
…		
Content	[1..1]	Content of the status report.
…		
POIComponent	[1..*]	*see section 1.3.2 Key Status*
…		
DataSetRequired	[1..1]	Data set provided in the related action of the management plan.
Identification	[1..1]	Identification of the set of key to download.
Name	[0..1]	Copy of *Action.DataSetIdentification.Name*.
Type	[1..1]	“SecurityParameters”
Version	[0..1]	Copy of *Action.DataSetIdentification.Version*.
CreationDateTime	[0..1]	Copy of *Action.DataSetIdentification.CreationDateTime*.
POIChallenge	[1..1]	A fresh challenge POI Challenge, generated by the POI
TMChallenge	[1..1]	The challenge TM Challenge 1 sent by the TM in the management plan.
SessionKey	[1..1]	
Identification	[1..1]	Temporary name used during Key Exchange
AdditionalIdentification	[0..1]	See *StatusReport*
Version	[1..1]	Temporary version used during Key Exchange
Type	[1..1]	See *StatusReport*
Function	[1..1]	“KeyExport”
ActivationDate	[0..1]	See *StatusReport*
DeactivationDate	[0..1]	See *StatusReport*
KeyValue	[1..1]	Key encryption key KEK, encrypted by the public key $K_{TM\text{-}Enc}$ of the TM.
ContentType	[1..1]	“EnvelopedData”
EnvelopedData	[1..1]	Encrypted key: Enc[$K_{TM\text{-}Enc}$](KEK)

This message may be protected in the *SecurityTrailer*:

- by a MAC (*AnthenticatedData*), if the POI own a shared symmetric MAC key,or
- by a digital signature (*SignedData*) of the message, signed by by the POI authentication key $K_{POI\text{-}Sig}$.

1.3.5 Configuration Update to Inject Keys

The TM sends a *AcceptorConfigurationUpdate* message containing the key to inject in the POI with following structure:

The Multiplicity in the following table should be considered to manage key download and not according to the definition of the protocol.

AcceptorConfigurationUpdate/ DataSet/Content	*Mult.*	*Usage*
HostCommunicationParameters	[0..*]	Cryptographic symmetric keys to download
ActionType	[1..1]	*see AcceptorConfigurationUpdate*
HostIdentification	[1..1]	*see AcceptorConfigurationUpdate*
Address	[0..1]	*see AcceptorConfigurationUpdate*
…		
Key	[0..*]	Identification of the symmetric keys shared between the POI and this host *see AcceptorConfigurationUpdate*
…		
SecurityParameters	[1..1]	Cryptographic symmetric keys to download
ActionType	[1..1]	*"Create"*
Version	[1..1]	*see AcceptorConfigurationUpdate*
POIChallenge	[1..1]	Challenge generated by the POI and sent in the *StatusReport* requesting security parameters data set.
TMChallenge	[1..1]	A second fresh challenge TM Challenge 2 generated by the TM to be sent by the POI in the *StatusReport* reporting the result of the security parameters data set download and installation.
SymmetricKey	[0..*]	For each symetric key to inject in the POI.
Identification	[1..1]	*see AcceptorConfigurationUpdate*
AdditionalIdentification	[0..1]	*see AcceptorConfigurationUpdate*
Version	[1..1]	*see AcceptorConfigurationUpdate*
Type	[1..1]	*see AcceptorConfigurationUpdate*
Function	[1..*]	*see AcceptorConfigurationUpdate*
ActivationDate	[0..1]	*see AcceptorConfigurationUpdate* The key is implicitly activated if absent.
DeactivationDate	[0..1]	*see AcceptorConfigurationUpdate*
KeyValue	[1..1]	Key to store Kxx, encrypted by KEK, sent in the status report.
ContentType	[1..1]	"EnvelopedData"
EnvelopedData	[1..1]	Encrypted key: Enc[KEK](Kxx) KEK key is identified by the Name "KeyEncryptionKey" and the Version of the SecurityParameter data set, provided in the Action of the management plan, truncated to 10 digits.

This message may be protected in the *SecurityTrailer*:

- by a MAC (*AnthenticatedData*), if the POI own a shared symmetric MAC key,or
- by a digital signature (*SignedData*) of the message, signed by by the TM authentication key $K_{TM\text{-}Sig}$.

1.3.6 Key Download Result

The POI sends a *StatusReport* message to report the result of the key download action with the following structure:

The Multiplicity in the following table should be considered to manage status of keys and not according to the definition of the protocol.

StatusReport/DataSet	*Mult.*	*Usage*
…		
Content	[1..1]	Content of the status report.
…		
POIComponent	[1..*]	*see section 1.3.2 Key Status*
Type	[1..1]	"SecurityParameters"
Identification	[1..1]	*see section 1.3.2 Key Status*
ItemNumber	[0..1]	*see section 1.3.2 Key Status*
ProviderIdentification	[0..1]	*see section 1.3.2 Key Status*
Identification	[1..1]	*see section 1.3.2 Key Status*
SerialNumber	[0..1]	see *StatusReport*
Status	[1..1]	*see section 1.3.2 Key Status*
VersionNumber	[1..1]	*see section 1.3.2 Key Status*
Status	[0..1]	*see section 1.3.2 Key Status*
ExpiryDate	[0..1]	Expiry date of the Key
Characteristics	[0..1]	Key detail, if the key has been downloaded.
KeyCheckValue	[0..1]	Result of the encryption of a null block: Enc[Kxx](00…00).
DataSetRequired	[1..1]	Data set to request a management plan.
Identification	[1..1]	*see ManagementPlanReplacement*
Name	[0..1]	*see ManagementPlanReplacement*
Type	[1..1]	*see ManagementPlanReplacement*
Version	[0..1]	*see ManagementPlanReplacement*
CreationDateTime	[0..1]	*see ManagementPlanReplacement*
TMChallenge	[0..1]	The challenge TM Challenge 2 sent by the TM in the *AcceptorConfigurationUpdate*, if the key download was successfull.
Event	[1..*]	Result of the action of downloading the secutity parameters.
…		*see StatusReport*

This message may be protected in the *SecurityTrailer*:

- by a MAC (*AuthenticatedData*), if the POI own a shared symmetric MAC key,or
- by a digital signature (*SignedData*) of the message, signed by by the POI authentication key $K_{POI\text{-}Sig}$.

Then the Terminal Manager sends a *ManagementPlanReplacement* message containing other action to perform.

1.4 Example

1.4.1 Introduction

The section provides an example of key download from a TM manager to a POI.

There are no symetric keys dedicated to this TMS communication loaded in the POI. Following a manual command or a response to a message requesting to contact the key injection server, the related TM must download an initial DUKPT key in the POI:

```
EE3AE644 1C2EEE18 3F3B4179 2DBCD318
```

with the following identification:

Message Item	*Value*
Keydentification	
KeyIdentification	SpecV1TestKey
KeyVersion	2010060715
KeyDerivation	398725A501E29020

1.4.2 RSA Keys and Certificate

There are 3 RSA keys:

For the POI, the authentication RSA key $K_{POI\text{-}Sign}$,

For the TM Host, the authentication RSA key $K_{TM\text{-}Sign}$,

For the TM Host, the key encryption RSA key $K_{TM\text{-}Enc}$,

To simplify the example, the public part of these 3 RSA keys are authenticated by the same certificate authority as described in the figure below.

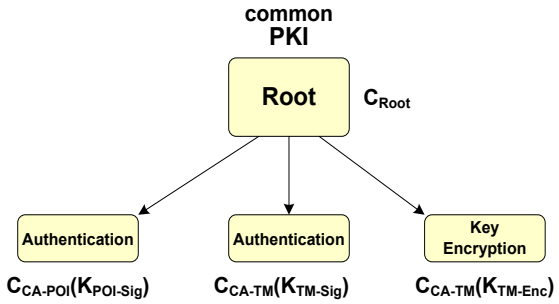

Figure 8: PKI used by the Key Download Example

282 The RSA root key to sign the certificates has a key length of 4096 bits with the components dumped
283 below:

RSA Key Component	*Value*
Modulus	A97F45122196E7353C89C240F5D163CF7B9B6A0899440C3D3F3C431BF898BFDE 121407E57E4B6EA2A85E52742659E05087CBC69E2EF6A301B9000A9DA4216951 B793B70B3D27EA9BD6E80584929C55AA5D315CF691F789E677E52105065CC79C 20C58384DF934640A80E7F970088650663610B80B478B17E5863B910332C89DF 3F1FEE47E8A96E9A413CD69410693FECBA0388D2DDB4B6B33341CF9D523AC561 729C5854512EDE984AEB1D937E3C8F74F527FFEFE710CBD2A6819CA0A3C8C7CB C237E1B60A66D790E5DFFCE5EF1B8BA241E284FBF32345AC74D179382DA7D714 E63CE04084FD904C3AAE0CAC44CCB17A4DFB4B5917971BE12B24FBC17E1E20DD DC363E45D1659C80D5FF087C51FBED5846C43C0D3580C1C7E8BE91629FDE96F7 A5E531E0166AFE88CC3AFE4EB642F9E51F02E007CB482B4E91D588965F53C73D 8CA2A2D4F7A8663F492CB1623906417A553C9D4DFB2CF55CE6290956C5E80009 7F0E8C974E879BCB981977377FA6A3750DBF478F57C0C7338F45BA83F54670E3 5DDBAC4E30665338A75C0D61DF6918721E885054C85BC3CACD2206468C8A84BB 8B3432CE2D8B2F46B3E25124E956E401AA4194066C01ADC9E633DD2BFE794C87 10F3B94766986465135B8B395F832166A17F9E7EDD8DCB0D19125307CC32B76B 7009113A1BD91C5A2815E0A5A533B8A6ABFC47F0D11A668A2791E9F2F6088A5D
Public Exponent	010001
Private Exponent	2329168FF34DD57A92AB55139AAAAC14CF6466F38FAFB1064786DDB900B1D723 5F06AEB8A9A1463B11C8373C86F41FF734A44DF8646F9F52ED28980B299010C3 F5DBFB9DA63B108CF160C23C45198F1FBF234D508CE917BF2A61EA9E9B3A45E2 1A5E3EB1229BEF77DC24DDCCDA3C7110892F096ED28132F8ADA74A2D9520091D B97F8B33798D2437758F044844BB409A7FDFD9D33C508F91CEF138FB3EA2986D 65940F32B6808D86740C1FDF87D1524505D21D628BC14D36CE79969F303AA74F 9A63733C0B1E585B63843A770C49DF86723A6631C9B7286DE4F1CB3E9F21F119 11C5D1133143545AABD58D2573442F10DAFA651FFF27C68DC8206CE52F9F5A5B B51BEDC9E488312A3B6FEB3C3F216C06B1DEAC0EEFBF0923146338A642D98136 45AD19BA6F057946FB7DD6C590E232ED8B7B41431D6970362F0D4DBCBD9B24E7 4C3B3339B312D350DF8CB61DED711FCDC184F06FB9D8F89E68BAC2ABBFADDF52 88946DE053723075CD4F429B413D7FD870A104145A6ACE893A20258864FAD2A8 6A1F5AD252269AF71283593929304F86D9720A43161E26ABA6B19E9E870B1B39 952B6D97EAA88904F8D5D33BC00C87AC207D30EB07FC90FC5EA1423AA7AED534 30DAA12A68E5FA78CC42336D34273F6530BFA098085990EA2A12252E68B5E166 67086DB85B22FF747ECC0AA74F3687A9C058ABF9B891CE423FDE410D6E3CE121
Prime 1	C68BEBAFB00F0A1B7150AB24BDFC6E9ACCB413951857EEF62EC81D78B7F4E432 CF653F969F81F6C26FB6ACC300302F583853C654B823E48EA617540F2EAE10A9 D46C005A539F270AFC86E8A1FDA9B66960B5C4B6D1746F5B616A6B90D8B1E822 C3AF0ED1097550D87B55C5B6651CBFE769A16051FAA4F416DEECBA79FD9252BC D99694FEA3981A50E329ECB367988A5FAEEB7C81FDAD8276B11CFC3AD0A85E65 53AB5D661EFA4D26A30157BD9FEA3428EB452F20D33525B2A9151BF542885B38 BF2FDAFA3CD3C3B48754822A5EF648D91A4CB3F98BCD222CC1497CB530A91B29 F1C52ED3F3242E1D6AB0A790708A3CB96D6DD718A7F1B4579EE6D0941DC06CE5
Prime 2	DA8B67A93CB27D2F5B7D2F86454FD2A57D20258058B3AE74999665E03C8A95A4 739D338B1312AD7E39EDBECADB3151A5172D198ABA2D1D6C88DFBA3462D52805 ADCF44070423098B0DC7D12CC767109860B1D1674F37CA2A3E03A425A76ECAB5 2737392460DB0221E90E099F02623FC93631E34C146B8DBD7367C0365C329704 C6D2304E0B4A8519737162556E0D36952D24A830DC8BDB1EDE7062C0DA000C26 44653F9F6043452EC676F51E3CF8EC2AC4B9249630CE522E2E754D5A0629612D 5D7180EBA39802E9DA665C6EA661A8483AB688D5B525B2EB0521BFF5E37211FA 7E882FE3F2FA109CC53800A902296BA6E4C3CCDC84E8EBAAB9EB59A03CCFC819
Exponent 1	9D26A8D1319865D69CD54DF1521358F45BEC78C77D3234A95513FE07CC0B2108 7A91D847FF4EDE22BE4BA7E8DCE046C91C246B0A2989F7615563879C50C563D9 1892B7A0C72964BCD46E6FF9B00EC19C1CF9228FD5AFC4685EEDDDE0133495D9 D66B5C5DE68F9E030B74337F0FFF36821360B11D923738205628A7DCE0F10D5D FF17AA2CF70DF05E6FBF8263EA2E99EFEC42E614F9D6793A3B2C0715028D11D2 3FEC968BBB1F412BC0BFD253FC1C6356B409D9A8B0A413879B3F6316B8A7B714 6E77916A99F4BFA5C7AC032F4864C5FA594FB6F0615067A96700249E41BAC80E 66183DDD734902DB33D4497D1126C9B3B742C68AF47B62D42BA8E415288B6365

Exponent 2	483FC1FB5F079AFF26FDD1D24FE3BDBDDC09DE9BF9B71D3B8AF2FFA70C1CBCAF EB50D3136D30C58E6F543BB91091D36E02A574463A9A6399D7FE2EAED6E5A51F 8B8073FAE5D1377C7307D60D39B6C6F3B933D0089955D64DF4C67B63BF608F3F 2841C770515CD5EDA4007209D15DEDBC756034C698119E803D40D578A32E4E62 D3DFF4FC381B60B933430EC1336AC6DAB65BE2069542DF23EB61B8240D6DEA96 54122CE061909BB485041AB0EE735490270D161D58F13C95EBE1F7BA8542F4CF 6C8EF391F33973ED1FB8AB62213B33C8FD300F38A774591BFD4C550BD32F88E6 0922B8C261376E7A8570A8373771BE172495DE8A209E681ABEF0216729F37F31
Coefficient	6978A387C201384A23F0E0BCD73737787364460ACF34F2B103AE60181A3E2DAF D4F26B819F4B1ED7CD9E8CF225922365ACFB408ACC2E87207E339CF72059B94B 09552BFFAED96E486CE29AABDC8B95DA948B19F26CE702FD4D40867B50F5CFF5 7361BD181A7B4AFF4D80C547A5CBF9D2D51E9A1D1C729FF12E84129DCB132DC9 DCEE79F45456A05F232E1B3C31CA02D56EBDBC031C81A85DDE3CA2A5E4CD2F5B C7D6394AA7F20022B74ED11A730C8C7024053C36500658D10C0622668C41E627 AF714A6EB76BCDC0B888F8AB4046DC5F158D08A5D7F388C76C7F022CE1834FDE 2B443126A9209274DED029D7D4FF7AC4B5AB0C88E8DEFD592D440AE254FBB422

The root X.509 certificate contains the following information:

Certificate Information	*Value*
serialNumber	5087 CBC6 9E2E F6
Issuer	
Country Name	BE
Organisation Name	EPASOrg
Organisation Unit Name	Technical Center of Expertise
Common Name	EPAS Protocols Test CA
Validity	
notBefore	20130418084958+0100
notAfter	20181001182005+0200
Subject	
Country Name	BE
Organisation Name	EPASOrg
Organisation Unit Name	Technical Center of Expertise
Common Name	EPAS Protocols Test CA
Extensions	
keyUsage	KeyCertSign CRLSign
basicConstraints	3

The dump of the X.509 certificate C_{Root} is:

```
0000  30 82 05 7D 30 82 03 65 A0 03 02 01 02 02 07 50  |0..}0..e.......P|
0010  87 CB C6 9E 2E F6 30 0D 06 09 2A 86 48 86 F7 0D  |......0...*.H...|
0020  01 01 0B 05 00 30 68 31 0B 30 09 06 03 55 04 06  |.....0h1.0...U..|
0030  0C 02 42 45 31 10 30 0E 06 03 55 04 0A 0C 07 45  |..BE1.0...U....E|
0040  50 41 53 4F 72 67 31 26 30 24 06 03 55 04 0B 0C  |PASOrg1&0$..U...|
0050  1D 54 65 63 68 6E 69 63 61 6C 20 43 65 6E 74 65  |.Technical Cente|
0060  72 20 6F 66 20 45 78 70 65 72 74 69 73 65 31 1F  |r of Expertise1.|
0070  30 1D 06 03 55 04 03 0C 16 45 50 41 53 20 50 72  |0...U....EPAS Pr|
0080  6F 74 6F 63 6F 6C 73 20 54 65 73 74 20 43 41 30  |otocols Test CA0|
0090  2A 18 13 32 30 31 33 30 34 31 38 30 38 34 39 35  |*..2013041808495|
00A0  38 2B 30 31 30 30 18 13 32 30 31 38 31 30 30 31  |8+0100..20181001|
00B0  31 38 32 30 30 35 2B 30 32 30 30 30 68 31 0B 30  |182005+02000h1.0|
00C0  09 06 03 55 04 06 0C 02 42 45 31 10 30 0E 06 03  |...U....BE1.0...|
00D0  55 04 0A 0C 07 45 50 41 53 4F 72 67 31 26 30 24  |U....EPASOrg1&0$|
00E0  06 03 55 04 0B 0C 1D 54 65 63 68 6E 69 63 61 6C  |..U....Technical|
00F0  20 43 65 6E 74 65 72 20 6F 66 20 45 78 70 65 72  | Center of Exper|
0100  74 69 73 65 31 1F 30 1D 06 03 55 04 03 0C 16 45  |tise1.0...U....E|
0110  50 41 53 20 50 72 6F 74 6F 63 6F 6C 73 20 54 65  |PAS Protocols Te|
0120  73 74 20 43 41 30 82 02 22 30 0D 06 09 2A 86 48  |st CA0.."0...*.H|
0130  86 F7 0D 01 01 01 05 00 03 82 02 0F 00 30 82 02  |.............0..|
0140  0A 02 82 02 01 00 A9 7F 45 12 21 96 E7 35 3C 89  |........E.!..5<.|
```

```
0150  C2 40 F5 D1 63 CF 7B 9B 6A 08 99 44 0C 3D 3F 3C  |.@..c.{.j..D.=?<|
0160  43 1B F8 98 BF DE 12 14 07 E5 7E 4B 6E A2 A8 5E  |C.........~Kn..^|
0170  52 74 26 59 E0 50 87 CB C6 9E 2E F6 A3 01 B9 00  |Rt&Y.P..........|
0180  0A 9D A4 21 69 51 B7 93 B7 0B 3D 27 EA 9B D6 E8  |...!iQ....='....|
0190  05 84 92 9C 55 AA 5D 31 5C F6 91 F7 89 E6 77 E5  |....U.]1\.....w.|
01A0  21 05 06 5C C7 9C 20 C5 83 84 DF 93 46 40 A8 0E  |!..\.. .....F@..|
01B0  7F 97 00 88 65 06 63 61 0B 80 B4 78 B1 7E 58 63  |....e.ca...x.~Xc|
01C0  B9 10 33 2C 89 DF 3F 1F EE 47 E8 A9 6E 9A 41 3C  |..3,..?..G..n.A<|
01D0  D6 94 10 69 3F EC BA 03 88 D2 DD B4 B6 B3 33 41  |...i?.........3A|
01E0  CF 9D 52 3A C5 61 72 9C 58 54 51 2E DE 98 4A EB  |..R:.ar.XTQ...J.|
01F0  1D 93 7E 3C 8F 74 F5 27 FF EF E7 10 CB D2 A6 81  |..~<.t.'........|
0200  9C A0 A3 C8 C7 CB C2 37 E1 B6 0A 66 D7 90 E5 DF  |.......7...f....|
0210  FC E5 EF 1B 8B A2 41 E2 84 FB F3 23 45 AC 74 D1  |......A....#E.t.|
0220  79 38 2D A7 D7 14 E6 3C E0 40 84 FD 90 4C 3A AE  |y8-....<.@...L:.|
0230  0C AC 44 CC B1 7A 4D FB 4B 59 17 97 1B E1 2B 24  |..D..zM.KY....+$|
0240  FB C1 7E 1E 20 DD DC 36 3E 45 D1 65 9C 80 D5 FF  |..~. ..6>E.e....|
0250  08 7C 51 FB ED 58 46 C4 3C 0D 35 80 C1 C7 E8 BE  |.|Q..XF.<.5.....|
0260  91 62 9F DE 96 F7 A5 E5 31 E0 16 6A FE 88 CC 3A  |.b......1..j...:|
0270  FE 4E B6 42 F9 E5 1F 02 E0 07 CB 48 2B 4E 91 D5  |.N.B.......H+N..|
0280  88 96 5F 53 C7 3D 8C A2 A2 D4 F7 A8 66 3F 49 2C  |.._S.=......f?I,|
0290  B1 62 39 06 41 7A 55 3C 9D 4D FB 2C F5 5C E6 29  |.b9.AzU<.M.,.\.)|
02A0  09 56 C5 E8 00 09 7F 0E 8C 97 4E 87 9B CB 98 19  |.V........N.....|
02B0  77 37 7F A6 A3 75 0D BF 47 8F 57 C0 C7 33 8F 45  |w7...u..G.W..3.E|
02C0  BA 83 F5 46 70 E3 5D DB AC 4E 30 66 53 38 A7 5C  |...Fp.]..N0fS8.\|
02D0  0D 61 DF 69 18 72 1E 88 50 54 C8 5B C3 CA CD 22  |.a.i.r..PT.[...."|
02E0  06 46 8C 8A 84 BB 8B 34 32 CE 2D 8B 2F 46 B3 E2  |.F.....42.-./F..|
02F0  51 24 E9 56 E4 01 AA 41 94 06 6C 01 AD C9 E6 33  |Q$.V...A..l....3|
0300  DD 2B FE 79 4C 87 10 F3 B9 47 66 98 64 65 13 5B  |.+.yL....Gf.de.[|
0310  8B 39 5F 83 21 66 A1 7F 9E 7E DD 8D CB 0D 19 12  |.9_.!f...~......|
0320  53 07 CC 32 B7 6B 70 09 11 3A 1B D9 1C 5A 28 15  |S..2.kp..:...Z(.|
0330  E0 A5 A5 33 B8 A6 AB FC 47 F0 D1 1A 66 8A 27 91  |...3....G...f.'.|
0340  E9 F2 F6 08 8A 5D 02 03 01 00 01 A3 20 30 1E 30  |.....]...... 0.0|
0350  0B 06 03 55 1D 0F 04 04 03 02 01 06 30 0F 06 03  |...U........0...|
0360  55 1D 13 04 08 30 06 01 01 FF 02 01 03 30 0D 06  |U....0.......0..|
0370  09 2A 86 48 86 F7 0D 01 01 0B 05 00 03 82 02 01  |.*.H...........|
0380  00 68 D3 BC 80 13 AC BC E2 14 B4 21 15 E8 C6 FF  |.h........!....|
0390  DF E7 86 7D C7 03 5F 6E 2D 16 42 8F 61 03 EB CA  |...}.._n-.B.a...|
03A0  1E E6 60 3B AA 4D AC FB 48 8E 00 3C 40 E9 48 48  |..`;.M..H..<@.HH|
03B0  3D EE C3 28 C2 F1 C4 68 D0 59 4F 9D 0B 31 50 37  |=..(...h.YO..1P7|
03C0  9E BB 7C 29 8B D9 C9 15 FE D0 D8 B2 1E 03 2B 56  |..|)..........+V|
03D0  EC 13 C2 11 F7 9E F3 A9 A0 90 62 C9 3E B4 09 9A  |..........b.>...|
03E0  8F A2 5E 91 EE 04 D8 CF 94 6B D3 0D 27 49 ED 1D  |..^......k..'I..|
03F0  DF 0C AB E9 95 CD 4D B7 12 8B 9B B0 29 FE 9C 77  |......M.....)..w|
0400  2F 5A 84 44 48 16 44 00 5C 23 B9 97 BE 94 75 FB  |/Z.DH.D.\#....u.|
0410  AB 54 CF AE D7 8C 96 4D CD FA E4 B8 C4 9F D9 BB  |.T.....M........|
0420  00 7A AD E0 AE E6 DC 3B 08 E7 E8 B7 62 EA A0 7F  |.z.....;....b...|
0430  9C 68 20 11 B2 A4 30 8D 35 15 3F A7 AB 2D 8E 29  |.h ...0.5.?..-.)|
0440  A3 28 00 0A 1E 1D 10 CC ED F6 F7 FB 12 AC 33 0C  |.(............3.|
0450  F5 AA 35 E3 78 77 26 42 14 40 CF C6 64 A5 98 81  |..5.xw&B.@..d...|
0460  07 1C 46 3A 3B 38 E4 E1 73 CE F3 D3 7A 0A DB D5  |..F:;8..s...z...|
0470  C9 F7 93 22 2A 3B 83 BD DD 68 D3 0D 8F D2 13 87  |..."*;...h......|
0480  FB C2 9B 29 94 0B 4A 91 A8 46 8B 16 C0 9A B7 2E  |...)..J..F......|
0490  74 D8 EB 41 3C 16 7A 28 3C 44 1A D4 B8 2E F8 6A  |t..A<.z(<D.....j|
04A0  29 6B 46 1B B7 91 45 0F 78 EA 83 B3 AD 92 BB 00  |)kF...E.x.......|
04B0  6B 42 5A 5E D6 DC DD 5C 58 EC E4 A4 D6 00 F0 68  |kBZ^...\X......h|
04C0  4C 47 79 5C 81 70 17 CE 50 FE 03 29 34 95 F9 45  |LGy\.p..P..)4..E|
04D0  C4 AC B9 CE 2A 76 22 4F 81 66 76 E5 46 83 0A E5  |....*v"O.fv.F...|
04E0  8A E0 35 1B C5 CD 17 14 1E 82 8B 7B B2 5C 02 87  |..5........{.\..|
04F0  33 27 0E E1 62 6B 4B 6A 01 F5 28 EC C3 A0 19 B9  |3'..bkKj..(.....|
0500  E6 9B 7A EB A3 ED 4B E2 04 38 74 FA 91 0C 3D 3D  |..z...K..8t...==|
0510  1F E3 6E D3 0B 8C 10 6D E2 C1 CB CB DC 3A 53 15  |..n....m.....:S.|
0520  E9 D7 B0 2B D1 AD 7D 81 20 67 23 4B 31 67 E4 8F  |...+..}. g#K1g..|
0530  9A 6C 8B 93 DA 33 A9 33 AB AE 8A BE EA 1C 3E 13  |.l...3.3......>.|
0540  C9 68 F4 E7 07 78 93 CE D3 A4 D0 7C 68 70 D4 78  |.h...x.....|hp.x|
0550  4D AF A0 12 F8 EA A9 A8 7F 5E DE 19 0E 0C BE 45  |M........^.....E|
0560  D3 36 5B 6A AC 5C 0F 6A 01 A4 4F 4B AD AA 1A 9A  |.6[j.\.j..OK....|
0570  06 33 91 46 71 EC 44 A7 93 70 8B 6B 2B 2E 00 87  |.3.Fq.D..p.k+...|
0580  B6                                               |.               |
```

The POI RSA authentication key $K_{POI\text{-}Sign}$ to generate the digital signature has a key length of 2048 bits with the components dumped below:

RSA Key Component	*Value*
Modulus	C22511390B85DB3990A27638B850616C18B11BDF78494B48B61F8F8D032225A8 FB00071293D4641C3CDDE18D47337EB7381AC12976820FF5C0B321E4EDF88C9B 8F16270E0FC6FAB470449BA70B947139551ABE326686F538C4F7F63A45FF4CB9 E6647000B28B791E1205ADB6ACDC29854698D90ACC3B6C84F0F8C2EFBEE4E3F9 844BD79AB14C1F22376198C13BEAC560DDC835104176729C7E62FBF4EC350DE4 D385C48D3EA40A90D7AA5838FAED3E3C760D19BB84D1997077C72331F3ADF050 B41DB5FFD19D129E88C75331DA13264BE4C2F0B0A0AA09F77EED2C801FAD239E 8FE5D8B43F10708FC3D6054B9156C5B55184F1A294DAB8F8267162BE9BB54867
Public Exponent	010001
Private Exponent	1F11BF87D9883A6523F85BE307DC153B2F58689582B27811D2D38A2D8EEAD00C 12DF1642AAD5BA8FAA4DF7E29C1A6994F8AD8F6C0B43153AC6F3E3E0B714A7AB DD62362DD1E88E068250F877EB2A7E542682791DA7BAC153AC71E23DC125F229 6DED74DF27B39A566D9BEB08E8F0F2D419502CABC5B35CD2899DC5D48840291B 65D1825915B19EC667600AF9EC1F677D2F9D8D5C54DFDAAF316FD291706361C2 852CA6DF00A651BC043312059F37891B7C83F66414E692DA58AD9A0DA19AF9BE 167F3A4CDC60618AF309565345D0B5D699208F84CA07ECDC5F1A082FB54791DD 03F4B3689738C821C824047F5C9441D112BBC9DF909724D5359956AE546AAA41
Prime 1	EBAB12EB45E933B2062E1FC1AAF81A987844DD504B10D4B493EAC90AD3882284 4DF24AA38F2C08C59FDE8FCBD80EC75E507B66A032FA7965A0EBF387BC75691E C0BC961C5A24E12D894ACEEA239C0320F52CD034276D746691EC2652115157BD B222A8B040DCE87731793A86BE01A00D31108135259F560C48B256521C73A3F3
Prime 2	D2E4E9EB2BDB7CEA1618A9C49DCDAC3BA0CEFC832DC06DB281A21597D0B2B9A2 5AA2FFC78654FECEC883937DB43847EDD391A0F209867BFE0F7C69C6D4CA1E4F 0A4AA6229249F6F961685EDEF250F86B9884256EC44D03980DD934CEA16A4471 9D79F9FDE018999B977E43F31412FD4D04FF8E06DB718A10848B0085388B4ABD
Exponent 1	673260747A06A6467C825211A266466F21AB362664D897EC0321BAAB6CF99DF3 C59625ACFD92D0BC8947123CB6FDB1BBD10E58602A32985A325F6022BE19C3D0 5DA1B731EF1F5B236F8D3C9236C9A86D142F6D7489175AF3574ECB710078582D 8F05B24C8BFAB0291196FE53E67C1BB3EB1A491A16C17112ABFABBE5F4E38695
Exponent 2	D006EA0F0635FDA3D2A4056262DEAC542D2DBFBB8DF7D0BD524E15CAA91C832C 79076C12DE991CB7D0E6A928480B74384E87CA20B5F0A88255B83D86DA037D9E 2DE2B0BA4D5F1475ADF60C0F132B77C07AB36F5131E55DF43144DE682CA4EC5A BE21C1CD01AE82670E2A88D0502EE3198422A9706E2A332C53F1E15388112E69
Coefficient	389861E483F93CA0FC53D9D73FCC8C28F5F1213ECE23D23B9A6F8E546BC8C0A8 C16ECE7A75F4CB1056F07638FBA8D4040AEB6AFA005102B06C243E67FA317B66 4E587BFC0F4481017E06D6669096805B043CB806503FB703DF1D31550E591659 35DE699BF055426A490333EAA4AA88A1C7F05106813340D6EB0398A2565E0310

This RSA public key $K_{POI\text{-}Sign}$ is authenticated by a certificate authority with the X.509 certificate $C_{CA\text{-}POI}(K_{POI\text{-}Sign})$ containing the following information:

Certificate Information	*Value*
serialNumber	2225 A8FB 0007 1293 D464 1C3C
Issuer	
Country Name	BE
Organisation Name	EPASOrg
Organisation Unit Name	Technical Center of Expertise
Common Name	EPAS Protocols Test CA
Validity	
notBefore	20130418102546+0100
notAfter	20181001182005+0100
Subject	
Country Name	FR
Organisation Name	EPASOrg
Organisation Unit Name	Technical Center of Expertise
Common Name	EPAS Protocol Test Client Authentication
Extensions	
keyUsage	DigitalSign

The dump of the X.509 certificate $C_{CA\text{-}POI}(K_{POI\text{-}Sign})$ is:

```
0000  30 82 04 83 30 82 02 6B A0 03 02 01 02 02 0C 22  |0...0..k........"|
0010  25 A8 FB 00 07 12 93 D4 64 1C 3C 30 0D 06 09 2A  |%.......d.<0...*|
0020  86 48 86 F7 0D 01 01 0B 05 00 30 68 31 0B 30 09  |.H........0h1.0.|
0030  06 03 55 04 06 0C 02 42 45 31 10 30 0E 06 03 55  |..U....BE1.0...U|
0040  04 0A 0C 07 45 50 41 53 4F 72 67 31 26 30 24 06  |....EPASOrg1&0$.|
0050  03 55 04 0B 0C 1D 54 65 63 68 6E 69 63 61 6C 20  |.U....Technical |
0060  43 65 6E 74 65 72 20 6F 66 20 45 78 70 65 72 74  |Center of Expert|
0070  69 73 65 31 1F 30 1D 06 03 55 04 03 0C 16 45 50  |ise1.0...U....EP|
0080  41 53 20 50 72 6F 74 6F 63 6F 6C 73 20 54 65 73  |AS Protocols Tes|
0090  74 20 43 41 30 2A 18 13 32 30 31 33 30 34 31 38  |t CA0*..20130418|
00A0  31 30 32 35 34 36 2B 30 31 30 30 18 13 32 30 31  |102546+0100..201|
00B0  38 31 30 30 31 31 38 32 30 30 35 2B 30 31 30 30  |81001182005+0100|
00C0  30 7A 31 0B 30 09 06 03 55 04 06 0C 02 46 52 31  |0z1.0...U....FR1|
00D0  10 30 0E 06 03 55 04 0A 0C 07 45 50 41 53 4F 72  |.0...U....EPASOr|
00E0  67 31 26 30 24 06 03 55 04 0B 0C 1D 54 65 63 68  |g1&0$..U....Tech|
00F0  6E 69 63 61 6C 20 43 65 6E 74 65 72 20 6F 66 20  |nical Center of |
0100  45 78 70 65 72 74 69 73 65 31 31 30 2F 06 03 55  |Expertise110/..U|
0110  04 03 0C 28 45 50 41 53 20 50 72 6F 74 6F 63 6F  |...(EPAS Protoco|
0120  6C 20 54 65 73 74 20 43 6C 69 65 6E 74 20 41 75  |l Test Client Au|
0130  74 68 65 6E 74 69 63 61 74 69 6F 6E 30 82 01 22  |thentication0.."|
0140  30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03  |0...*.H.........|
0150  82 01 0F 00 30 82 01 0A 02 82 01 01 00 C2 25 11  |....0.........%.|
0160  39 0B 85 DB 39 90 A2 76 38 B8 50 61 6C 18 B1 1B  |9...9..v8.Pal...|
0170  DF 78 49 4B 48 B6 1F 8F 8D 03 22 25 A8 FB 00 07  |.xIKH....."%....|
0180  12 93 D4 64 1C 3C DD E1 8D 47 33 7E B7 38 1A C1  |...d.<...G3~.8..|
0190  29 76 82 0F F5 C0 B3 21 E4 ED F8 8C 9B 8F 16 27  |)v.....!.......'|
01A0  0E 0F C6 FA B4 70 44 9B A7 0B 94 71 39 55 1A BE  |.....pD....q9U..|
01B0  32 66 86 F5 38 C4 F7 F6 3A 45 FF 4C B9 E6 64 70  |2f..8...:E.L..dp|
01C0  00 B2 8B 79 1E 12 05 AD B6 AC DC 29 85 46 98 D9  |...y.......).F..|
01D0  0A CC 3B 6C 84 F0 F8 C2 EF BE E4 E3 F9 84 4B D7  |..;l..........K.|
01E0  9A B1 4C 1F 22 37 61 98 C1 3B EA C5 60 DD C8 35  |..L."7a..;..`..5|
01F0  10 41 76 72 9C 7E 62 FB F4 EC 35 0D E4 D3 85 C4  |.Avr.~b...5.....|
0200  8D 3E A4 0A 90 D7 AA 58 38 FA ED 3E 3C 76 0D 19  |.>.....X8..><v..|
0210  BB 84 D1 99 70 77 C7 23 31 F3 AD F0 50 B4 1D B5  |....pw.#1...P...|
0220  FF D1 9D 12 9E 88 C7 53 31 DA 13 26 4B E4 C2 F0  |.......S1..&K...|
0230  B0 A0 AA 09 F7 7E ED 2C 80 1F AD 23 9E 8F E5 D8  |.....~.,...#....|
0240  B4 3F 10 70 8F C3 D6 05 4B 91 56 C5 B5 51 84 F1  |.?.p....K.V..Q..|
0250  A2 94 DA B8 F8 26 71 62 BE 9B B5 48 67 02 03 01  |.....&qb...Hg...|
0260  00 01 A3 0F 30 0D 30 0B 06 03 55 1D 0F 04 04 03  |....0.0...U.....|
0270  02 07 80 30 0D 06 09 2A 86 48 86 F7 0D 01 01 0B  |...0...*.H......|
```

```
0280  05 00 03 82 02 01 00 54 0D B4 CC CA 78 C5 B7 2E  |.......T....x...|
0290  C3 4D 6A 55 EE 7C 15 2E D5 44 09 41 9E 0B 7B C7  |.MjU.|...D.A..{.|
02A0  83 B8 55 95 57 C0 2C CA 5E 81 B6 CC A8 54 A3 62  |..U.W.,.^....T.b|
02B0  50 AD CA 0C D5 5C 96 F4 2F 01 97 99 B5 A1 00 C9  |P....\../.......|
02C0  72 D3 F2 41 1C B2 67 63 00 F1 B0 9E 46 AE 4F 29  |r..A..gc....F.O)|
02D0  3A 24 CB 71 EE A5 46 7C B9 19 33 71 3E 55 6F FC  |:$.q..F|..3q>Uo.|
02E0  C0 B5 58 DA 34 4F F4 F8 AB 30 A2 F8 03 BD 97 BB  |..X.4O...0......|
02F0  56 81 00 BA C6 B6 FA E8 84 F8 31 BF 85 5C 4E E8  |V.........1..\N.|
0300  23 FE 3B AC 3B A2 D8 B6 15 F6 2C 1C 16 85 B9 BC  |#.;.;.....,.....|
0310  59 DF CB E1 CF BD FD B2 9F 37 73 FD 46 68 56 88  |Y........7s.FhV.|
0320  BF 65 66 70 F5 BB 9C E5 6B 02 9E 36 E7 29 16 29  |.efp....k..6.).)|
0330  DE 69 FA 85 83 67 61 9D 8D E4 FB 9F 08 60 85 18  |.i...ga......`..|
0340  85 A4 28 94 AD C9 7D CB 51 D4 CE BF 9F 52 08 3D  |..(...}.Q....R.=|
0350  D5 11 37 1B 15 7E 3D 16 F9 34 69 EE D0 B7 FF 01  |..7..~=..4i.....|
0360  BC 13 7D 50 65 E2 66 A8 EA 3C 82 99 9E F3 62 63  |..}Pe.f..<....bc|
0370  A8 63 ED 5F E2 2A 69 E4 87 4F DF 41 A1 9F A4 57  |.c._.*i..O.A...W|
0380  B1 2C F6 A5 2B 08 F7 3B D3 BD 9C 2F D1 33 52 EC  |.,..+..;.../.3R.|
0390  EE 4E EF 63 23 82 6B F7 24 40 FC 14 9E BD 58 91  |.N.c#.k.$@....X.|
03A0  A8 D6 D0 E5 DA 50 54 77 08 52 5C A4 02 1B 51 05  |.....PTw.R\...Q.|
03B0  9B 52 B5 0E 61 B1 76 C1 F9 62 AA 7A C2 80 99 34  |.R..a.v..b.z...4|
03C0  31 DD 5B F3 D6 C1 46 AD BA 76 2B 3E 67 29 F1 7F  |1.[...F..v+>g)..|
03D0  A6 39 D9 8D 5C BF DC AE 55 6A 2F C0 B2 37 54 E4  |.9..\...Uj/..7T.|
03E0  91 F9 7B F1 7A 18 D8 42 A8 7F 8D E4 FB A5 8B 56  |..{.z..B.......V|
03F0  51 72 13 BC 59 C5 12 D4 F0 44 7F 0C 19 7B 38 78  |Qr..Y....D...{8x|
0400  5A 45 7E 0A 0E 7D D4 48 06 C4 BA 16 F8 11 B7 A2  |ZE~..}.H........|
0410  50 24 79 1E D7 42 E7 43 92 C9 D4 BA BA 75 4F 09  |P$y..B.C.....uO.|
0420  B6 1D D8 EC 2A BB F6 73 7E 49 2B BC 37 18 50 72  |....*..s~I+.7.Pr|
0430  AC 9E BE A3 DE F2 FB D5 6E 83 6B 88 D0 80 9F 96  |........n.k.....|
0440  A4 B2 AC A1 A5 B5 9D 19 8F 94 99 0B A4 D2 A1 B5  |................|
0450  0C F6 4C 5E 83 91 D6 DC AD B5 8C 9E 07 4E 60 8D  |..L^.........N`.|
0460  7D 01 23 09 A9 2F FD CE FD 96 CD AE A4 F6 BE 5E  |}.#../.........^|
0470  57 2A 20 16 1C 3D 6F D8 38 FF AE 96 6B B2 C6 71  |W* ..=o.8...k..q|
0480  E7 C8 36 FB 36 9C 28                             |..6.6.(         |
```

The TM Host RSA authentication key $K_{TM\text{-}Sign}$ to generate the digital signature has a key length of 3072 bits with the components dumped below:

RSA Key Component	*Value*
Modulus	BD095898F981BAF42BE20E19339B396C59626690BDF396D20C503CA57C688AF4 1E50552CF1B9DDC4116209DD00C26B673F7EDEE7D0CA6DC2DAA9FF2F8C3A860B 8F835AE60D9E057EDDF1625FAC55A102837FC1C7EF8C0A6C137C5973972ABC40 F4D482F5EBC9754F964B6EECEDBE66DB62AD0DA7B38E05917562E899DF717D27 457693B41E7BF2CBA98855AE2C97DE4B48FD812A520D6D356010F6E8355EC98D BA3047F2C0CDCD9BE655277F3ED69A788DD80A6A12BCA3D4C7F08662B99D3F70 A9548D7804B5E4A2913A3EC02525BE639ED7D9B986556C5932675642FCC4E659 D828A94C5544AEBBC5446EE6B96A04A0185470296DFC2FFBA73D4074930968DD 810E43D574DD7BE664899DA6E48EB4B3B590E2CAA97C75015C735093AD62E3FD 791AB5718F1FA19673EBAF7ABF3CCD732F31D397FCE790869D2A682DF2324514 181CCE1CDB4E7A4036DABAC26276EE0A3A2D2BE04FB52E58128FF4086C7417CD ECE75B18783DFA2C05D4A51899307FDCC4A00701300D73B45FFD52E396758CC5
Public Exponent	010001
Private Exponent	17D112A18B6605E8F7926E964C433553EA5B14730E0B9FA7ED373ABCDAD4CD14 FEB0BE5A80461BA3B550F5CF2B665363D9C3215071A4DF795A556ABA51DF99BD E121FA94DB885A46E6AD9FE84FED25F10C224F86E22E71ADB632C78E61B057B1 936726ECD6FD35D3862B10D9B706732D16DC98C8D53D82841617151935E6B58E FA187B798911B2C06826AE2CD89F75B96483D3FF4201410E25815DAA59F70C4B D7F6774A2572888228DDF7B0F778D0537A038B245C21FA3E37C69D17D92CEFAE 0999568D7ED81EE98DD3529FD19C52E890CABB99538A8AAD768E2CA7A1F2191A 8A4C0D1C1431A90C7A8AD3240349E7B30344E9F946EBF9CA556B1348936C04C0 24D45C87204F7E04C828A6A781085E5541451C4111A0AA63F807E32D0F941611 8E9F395E936D5AE530F490B05F76337B4AD6C79CACBFB65A12BC137A5B98F02B 8E7456A123F4C43AC50E2244344A3D86402B74E2A66A28EF69095D0A044D14D9 E164F9F67561B462EB95B65A6298BA636BD9E4A150D02357FB293F0B5CF0C5AD
Prime 1	E67D8DC159476C2CB803BA39BBF3606B3F45434FC07AF91368406B57095D205B AC88BFAF9462B458F9B4DCC26078B27040766510A19F317021AC87B5BDD618BE 95850BC5A895787F6D134C578F9218EAD686EFED14EAA84804F749794288E24C EA2A955AA3473EF99A0D536A7AA13E0DFAD7739A42F46C98C55C8066FBA20EDB 91D587A966F061351A46141CEBCFD944E766FBCAA19F251A09BF6BD7E3B8A8FD F3AD572B7B7FEC9B160C8F8A6FDE5E029D7942A45F5572BD40B04F3CF59F4BF7
Prime 2	D1F548FB2D1A25B094040F6B26B051F99F6E7C9DB34148A458393C08BC2232EB CDB9E98BD8CB7E1E1A5D133F668E535E1A27FAF807C253057438ADF7846AA656 7E03A4879248DF06A9A8E413F8125CAC14B2093EB043AB4831F16EF7DB04FD34 855D525A6C5BE4E7D2C6B6F02C97BF975BE971C5F8515BBE2FE9BD894B39DF74 CED4BE6BEEF5D35C5D420BDD29111EDCE556D1DC38669AC9D5136FAF44951381 BE2B1F51DD150EB1A591C46242E54715550710E7AB20BAFC50B6D31469F4A623
Exponent 1	5E579BD33D40DFC53A18C47BE7338A0EBBDA14E02AEFEACD87C97E6624BE0A85 9B8C69B16B722F518FFBF8B4531A7427402B75D8A5DEEC34728415144DBCB96A 20F751473966DCE88373F7B68B5C88786F10D259DF4AE150813FDAC2187AC0EE 2C96FB851AFA098BCF038F56311598B9CE27ABF8C3591AAE3972505856BD1189 CC1A73A9E22998104D4DCBE3BE9DD7D7BD43C8E23ADF5227634007DB5929777A 62E85B9ABFB52FDA96DED34E1DD60DF2D214153404958C1E6CC0FDDDFCC79427
Exponent 2	80A494A9E9B19AA43D9CDB41A0FBE9CE53E463905093D08979D0DFBACE62F9E6 4730012C0192755CC6747EE59AD5DBB8CDB7EF6AE77E26563226C458E3166182 9F45661AF703953B44DAC99C7EA3E98A3A47F7A82461E1E1A35035D8C1A6A5E9 F748FDBB8FA72272F44F732967793717EB65F6A3010A0077606E0C06C243DC69 7A8D197B9277A6A07237948356B539BEC8FA502D69955C840BFD13B245083E62 817D747C3944BCB3162A61347F9E71D65D39AE1EF4586299546F2097E26FD717
Coefficient	D175B7C635A4E77C5140848E541B1F75EF83ADEDF347B1727A332FC292142080 8225783A23F9475692A0E14425BEDD0CD72342F243AC24D0901778B91C58A9A2 515F72538BC0F1DC7167FF598247F1CE2A475967256AA3FA63EC1008C8B7FF90 51DF38D7B9B7AC0B86CBDFA141DC22D755898FB471818202734F761D3464C9B0 5E7F0119E80F7BD4F205233B020DB1EEA7CC8DE11BB68CF8A0F82CE8CD3E33C5 2472FC11229F8C0A56F85189D0B7868958E1987D7B7819EB85C5B05FB1CD0448

This RSA public key $K_{TM\text{-}Sign}$ is authenticated by a certificate authority with the X.509 certificate $C_{CA\text{-}TM}(K_{TM\text{-}Sign})$ containing the following information:

Certificate Information	*Value*
serialNumber	2ABC 40F4 D482 F5EB C975
Issuer	
Country Name	BE
Organisation Name	EPASOrg
Organisation Unit Name	Technical Center of Expertise
Common Name	EPAS Protocols Test CA
Validity	
notBefore	20130418100646+0100
notAfter	20181001182005+0100
Subject	
Country Name	FR
Organisation Name	EPASOrg
Organisation Unit Name	Technical Center of Expertise
Common Name	EPAS Protocol Test Host Authentication
Extensions	
keyUsage	DigitalSign

The dump of the X.509 certificate $C_{CA\text{-}TM}(K_{TM\text{-}Sign})$ is:

```
  0: 30 82 04 FF 30 82 02 E7 A0 03 02 01 02 02 0A 2A  |0   0          *|
 10: BC 40 F4 D4 82 F5 EB C9 75 30 0D 06 09 2A 86 48  | @      u0   * H|
 20: 86 F7 0D 01 01 0B 05 00 30 68 31 0B 30 09 06 03  |        0h1 0   |
 30: 55 04 06 0C 02 42 45 31 10 30 0E 06 03 55 04 0A  |U    BE1 0   U  |
 40: 0C 07 45 50 41 53 4F 72 67 31 26 30 24 06 03 55  |  EPASOrg1&0$  U|
 50: 04 0B 0C 1D 54 65 63 68 6E 69 63 61 6C 20 43 65  |    Technical Ce|
 60: 6E 74 65 72 20 6F 66 20 45 78 70 65 72 74 69 73  |nter of Expertis|
 70: 65 31 1F 30 1D 06 03 55 04 03 0C 16 45 50 41 53  |e1 0   U    EPAS|
 80: 20 50 72 6F 74 6F 63 6F 6C 73 20 54 65 73 74 20  | Protocols Test |
 90: 43 41 30 2A 18 13 32 30 31 33 30 34 31 38 31 30  |CA0*  2013041810|
 A0: 30 36 34 36 2B 30 31 30 30 18 13 32 30 31 38 31  |0646+0100  20181|
 B0: 30 30 31 31 38 32 30 30 35 2B 30 31 30 30 30 78  |001182005+01000x|
 C0: 31 0B 30 09 06 03 55 04 06 0C 02 46 52 31 10 30  |1 0   U    FR1 0|
 D0: 0E 06 03 55 04 0A 0C 07 45 50 41 53 4F 72 67 31  |   U    EPASOrg1|
 E0: 26 30 24 06 03 55 04 0B 0C 1D 54 65 63 68 6E 69  |&0$  U    Techni|
 F0: 63 61 6C 20 43 65 6E 74 65 72 20 6F 66 20 45 78  |cal Center of Ex|
100: 70 65 72 74 69 73 65 31 2F 30 2D 06 03 55 04 03  |pertise1/0-  U  |
110: 0C 26 45 50 41 53 20 50 72 6F 74 6F 63 6F 6C 20  | &EPAS Protocol |
120: 54 65 73 74 20 48 6F 73 74 20 41 75 74 68 65 6E  |Test Host Authen|
130: 74 69 63 61 74 69 6F 6E 30 82 01 A2 30 0D 06 09  |tication0   0   |
140: 2A 86 48 86 F7 0D 01 01 01 05 00 03 82 01 8F 00  |* H            |
150: 30 82 01 8A 02 82 01 81 00 BD 09 58 98 F9 81 BA  |0          X    |
160: F4 2B E2 0E 19 33 9B 39 6C 59 62 66 90 BD F3 96  | +   3 9lYbf    |
170: D2 0C 50 3C A5 7C 68 8A F4 1E 50 55 2C F1 B9 DD  |  P< |h   PU,   |
180: C4 11 62 09 DD 00 C2 6B 67 3F 7E DE E7 D0 CA 6D  |  b    kg?~    m|
190: C2 DA A9 FF 2F 8C 3A 86 0B 8F 83 5A E6 0D 9E 05  |    / :    Z    |
1A0: 7E DD F1 62 5F AC 55 A1 02 83 7F C1 C7 EF 8C 0A  |~  b_ U         |
1B0: 6C 13 7C 59 73 97 2A BC 40 F4 D4 82 F5 EB C9 75  |l |Ys * @      u|
1C0: 4F 96 4B 6E EC ED BE 66 DB 62 AD 0D A7 B3 8E 05  |O Kn   f b      |
1D0: 91 75 62 E8 99 DF 71 7D 27 45 76 93 B4 1E 7B F2  | ub   q}'Ev   { |
1E0: CB A9 88 55 AE 2C 97 DE 4B 48 FD 81 2A 52 0D 6D  |   U ,  KH  *R m|
1F0: 35 60 10 F6 E8 35 5E C9 8D BA 30 47 F2 C0 CD CD  |5`   5^   0G    |
200: 9B E6 55 27 7F 3E D6 9A 78 8D D8 0A 6A 12 BC A3  |  U' >  x   j   |
210: D4 C7 F0 86 62 B9 9D 3F 70 A9 54 8D 78 04 B5 E4  |    b  ?p T x   |
220: A2 91 3A 3E C0 25 25 BE 63 9E D7 D9 B9 86 55 6C  |  :> %% c     Ul|
230: 59 32 67 56 42 FC C4 E6 59 D8 28 A9 4C 55 44 AE  |Y2gVB   Y ( LUD |
240: BB C5 44 6E E6 B9 6A 04 A0 18 54 70 29 6D FC 2F  |  Dn  j   Tp)m /|
250: FB A7 3D 40 74 93 09 68 DD 81 0E 43 D5 74 DD 7B  |  =@t  h   C t {|
260: E6 64 89 9D A6 E4 8E B4 B3 B5 90 E2 CA A9 7C 75  | d            |u|
270: 01 5C 73 50 93 AD 62 E3 FD 79 1A B5 71 8F 1F A1  | \sP  b  y  q   |
```

```
280: 96 73 EB AF 7A BF 3C CD 73 2F 31 D3 97 FC E7 90  | s  z < s/1     |
290: 86 9D 2A 68 2D F2 32 45 14 18 1C CE 1C DB 4E 7A  |  *h- 2E      Nz|
2A0: 40 36 DA BA C2 62 76 EE 0A 3A 2D 2B E0 4F B5 2E  |@6   bv  :-+ O .|
2B0: 58 12 8F F4 08 6C 74 17 CD EC E7 5B 18 78 3D FA  |X    lt    [ x= |
2C0: 2C 05 D4 A5 18 99 30 7F DC C4 A0 07 01 30 0D 73  |,     0      0 s|
2D0: B4 5F FD 52 E3 96 75 8C C5 02 03 01 00 01 A3 0F  | _ R  u         |
2E0: 30 0D 30 0B 06 03 55 1D 0F 04 04 03 02 07 80 30  |0 0   U        0|
2F0: 0D 06 09 2A 86 48 86 F7 0D 01 01 0B 05 00 03 82  |   * H          |
300: 02 01 00 76 04 AD 89 65 54 B8 D7 1E 07 07 69 70  |   v   eT     ip|
310: E1 4C 3F 42 E6 63 8B 75 8E 50 C3 05 C3 E1 DD 8A  | L?B c u P      |
320: BC 3E CA 02 15 0A F5 10 1D 36 81 46 38 15 0E 4F  | >       6 F8  O|
330: A7 3E 5D 92 E5 79 98 3B 49 8B DA 29 FB E9 CE 14  | >]  y ;I  )    |
340: A7 93 F1 2F 5F B0 89 61 B7 3D C1 C8 3F B3 74 67  |   /_  a =  ? tg|
350: B2 C5 BA FF F6 1C F6 1B 79 36 38 EA 21 E3 41 8B  |        y68 ! A |
360: CA B5 C7 1E BA 20 25 23 0C EC F6 A0 B9 89 30 13  |      %#      0 |
370: F7 F5 B4 E6 64 19 A6 04 55 CC 90 C5 FE F5 96 B7  |    d   U       |
380: 6F A9 14 F3 5A DF E0 88 E1 52 5B 34 E1 C3 F1 19  |o   Z    R[4    |
390: 2B F8 1D 59 FF 67 F3 11 A1 F7 E6 14 E9 33 2F 9C  |+  Y g       3/ |
3A0: 6C EA 0D DB 9F 0C 0E EB 57 08 AC 2D B2 0F 01 7F  |l       W  -    |
3B0: 06 07 9A 1B 7C 03 25 4F 25 BB A1 3E 21 41 85 A0  |    | %O%  >!A  |
3C0: 56 7A AC 72 20 03 50 48 88 AB 4A 9F 5A CF D0 C3  |Vz r  PH  J Z   |
3D0: AC D4 D4 C3 C3 A7 5D 83 0B 96 B1 79 20 77 DD 6F  |      ]    y w o|
3E0: F0 0C 6F DA 53 CC B1 FA 6A 2F F1 C8 56 F7 79 8B  |  o S   j/  V y |
3F0: F8 31 32 F6 23 84 0F B2 12 E7 10 C6 FE 50 5A C6  | 12 #        PZ |
400: 45 38 03 83 E5 EB A7 EC CF 08 E2 26 22 CC D8 74  |E8         &"  t|
410: 8D D0 4C D6 EC DA 35 08 D8 3A 4D EB A9 6D 05 23  |  L   5  :M  m #|
420: DB 87 64 39 5E DA B5 9A 42 42 17 80 5B D8 D7 15  |  d9^   BB  [   |
430: F4 01 D5 44 27 27 B0 6D 07 CB C2 D6 05 E0 CA 4E  |   D'' m       N|
440: 47 F7 52 7A 3E 30 0E A6 96 75 EB 77 71 45 98 97  |G Rz>0   u wqE  |
450: 1B 26 53 DD 0B 73 40 43 36 5F AF A4 59 09 31 4A  | &S  s@C6_  Y 1J|
460: 85 FF B4 6B A3 4F 88 B2 28 E9 9D 53 73 9D 3F 00  |   k O  (  Ss ? |
470: E7 8D 3C EA DE E7 36 DA AE 11 5C E5 0A C1 0E BF  |  <   6   \     |
480: B0 AC 58 71 24 4B BA 07 11 07 1B 1E 40 FA 1C C6  |  Xq$K      @   |
490: 0E 12 58 D6 D4 97 88 F7 23 B1 4E 04 F4 8D 58 89  |  X     # N   X |
4A0: 82 61 C3 73 98 B5 51 0D C4 7F 5C 5E F6 D7 D2 7B  | a s  Q   \^   {|
4B0: 0C 80 F2 87 6F 2B 02 57 1C 8B AC E2 91 74 22 1B  |    o+ W     t" |
4C0: DC B5 64 70 42 B4 B6 7D F7 D1 31 E9 32 46 70 CB  |  dpB  }  1 2Fp |
4D0: 64 D2 E1 B1 59 77 D6 51 FC A4 8F EF 62 8E A2 B1  |d   Yw Q    b   |
4E0: 37 A9 23 6F EB 7C 34 E1 9D 8F DF 43 7C 84 08 A5  |7 #o |4    C|   |
4F0: 6C E0 62 B2 CC 43 5D 85 EC 65 A2 5D 8B 41 B5 12  |l b  C]  e ] A  |
500: 06 7C AB                                         | | |
```

The TM Host RSA key encryption key $K_{TM\text{-}Enc}$ to protect the key encryption key, has a key length of 3072 bits with the components dumped below:

RSA Key Component	*Value*
Modulus	D72CCF63FB2F866A18F219DC919316495FF66C906F904D7B266525C37FABE7D4 ED99EA0424336D99B0B7979DE1764E7CD16B64B9BA954610BCACBB6CFDA4CB90 6AA75BED58B9A0037152541EB1DC3DD0B6214EB31BE97A4F91073412DE042216 FA8F826D24C7F2D305D4BF63465BF899DC6F073FF6AA338EA44DB6BE51A6358C AA3CCB8528E58B55540ED22325233333D3D6D2B82ED7A58D499F445FF835C3EB D5B515379A7C2B5B41D35F3DFD5A1A2D61491038FDD19E18EF678FD794872ACC 8B8129AFA0D02FCD6E4ADE9184D5FEC2386441293B16BB76B8E2E4F8E8027636 6855A880E0EFAC449E76124C4BF7FF2BA15E674B62A5637D26600AA3A013E153 0E11F4BF984E533F520A2E74BD826DD507C283D2F563C22848E05D84D2B7D222 1F4B63B56797E6AFB425D567E5F916E3AB4E2C486EC81489469C17DA2DFAF7AB 496EE7C24E43951FFE28006BFF96E2D15838AC7252F3D45E8FEBEF0F7EEF974F FE0A38C38926CFA0683198CA8FD08C8B2427B91A0B16F79A7186DE7DAB9DFF3D
Public Exponent	010001
Private Exponent	70CA3357D446202E232F5CB10AB9D017DC2E7ECFE33AFFF24AB900678ED7DC68 F7B7133CE280F6B57635764B32F0E1C979B8D28EACA82C96FF5F87CB64D56A43 2434DFF1F4ED305C3D9D8B2C9FCCB3B66091EAFFE5E4A7D16753204FB782F11F 9C6D774FA0D5128ADCE69CFFFBD49FE67EEED01D0E3E3F5248FBD78BC19EDF39 01CF665B4189B9549C003CD461562733C69A37D085F551F9529B22AB2F9F7738 7AC835FBF4859BF074FBC853E526C2CC00CFDCAA131A3AC6154FF2CD6D34C110 8A903DDA424D8A689EBCCFDB05FCAC0B9FC16C3091D284506661F52D4A2FAB8C A519B79C882E1E1DA6E04BC292D8C86A073BBB4DD354FE9A068F59621AD2739C F0C7C1536187337B758F0CA31CE1381EC81D61EF92F7251BA60ABC2F3732C0CB 31979282D7B96866CAD0CFD4842A1041E2A8BC720FB2B9147DED36BAD36E323E 21482BD5A5416E3FA2DB23355B19A3534910DA8A03FC41B2DCA278796D98E9A3 BE44410361825CBA24ACC5E0D5276FE55A6AD20E0F8FE1F3BFBE7DC5E1D5F581
Prime 1	FA00B40D29723058B33EB625A4B52D9B9F010360F739135E4A6AB13A24780D7C D577657B3E6DB0043C4B1422384D4023E2F901B922D188C5AE0365B816DCF8AF 7E62E4ECF2D0AB3EA21B362B811873661BFF476DD123509F07D8D633CC373F7A EF59894385BF9FC7E82BBD84DC148922A00558DD365A47B6A384BF91EAF440F4 E05D4BC95481AEFB61A1706C1E4B62A482A0A5AE9E3A87ED64826896CDD52B00 355FDF2D81B649E553D412205C0EFB4E075C2526FDDFA885F94AAFA323C4601D
Prime 2	DC5639C6AE9A6BD28746623C4D86C4A4E0212A1BE44EC34054FEEC65C101DC1E 0F45183CEC4CECB367E250D69A1B4ADE858BD67CE8CDCFAE182369B7B86D2DC0 F1159429A29E1293ADAFC66C5A8673D789D589AA66D0C25AE6B5325D1477B47A 713DC43842E22A36AEB738A893D17CFEAC4F9F0FF25DCD5D7DAD3AF7346B88EA D4E5C86ECC970BC67BE142C53534788006AA1D8FADE91EE6D988BDB6D57775C7 3F8C41AAEF83508E836A92083B571D52E2904D0592A34900787C9650A41831A1
Exponent 1	D72FA7CAF473BF3D79FB6E98F42EA6B51EA5A69CDDEF18C6BE531B7D2A4AD381 31D4755B219F14347119469935D0F8766B355DD05731F801FF081993DCCA129C 2BB33FCCDC2BD45A32FA2D24411824AC2D490BD8707D6F35937186DE4AD6FB22 FBC61BAA2D0385AA7222C41C09BAFB56FC59DDE57A9536C8F3F29D5A21DC5FD4 E71226DB828BA56BE6DB2883478827BDE65A14823ADBB288194D4E6D0F7A7E6A CD8659F9377F0A180491B3907AECC24EA57320DF710204725CE3764E7BC8D9D9
Exponent 2	5826F73E92249DF6C0C05C151C3F4AF55BE668DE77DD3B28C5D8A7E39DF08C8C 4A37AE96D143857FD1942E1B6DD47583C99244E1FC923B00C00F8B0041FD0C4D 21272CFBEB5FAAB702CA4C6C955B2D859253A89C503E3D43F9018D80C7EB8C7D 604901F4306E23CD74E140FDD106032830F03A073B4464217F628B30D3FC21EF 31F62CD6876BF6FE1619ED88D0DC89494F61482A6FBDD0EB33250E21D40DD345 401B713A5E50FF2DC54E21D6C146FD286814AB7C0B4AE0AE1B865CED2E79AF81
Coefficient	BF2571D99CCC8D31ECEE0DE36E8C591043C371D01052AE0DF46DD35118031F5E 4AAB2948761A9BFCE909047EA5143B03EAD08A65B9F0E96F525ABF014A121E4C E7935EDB7F0244357B1E20E106066A2E0BF326D82BFE6EDD2A283174D6E9A865 D3FD60D3FACC1D1B8F82FD32A9DAE2CEFC92C0BA4A3D66872A82FB1E67608565 3EDF96B096766729824F4C2B050494C7CE6ADEE376379558E3DA58CC608558CD A2C4257398C03A973B9790ADAE2E3D4FD18A551DBC847E632455BB55633698EF

This RSA public key $K_{TM\text{-}Enc}$ is authenticated by a certificate authority with the X.509 certificate $C_{CA\text{-}TM}(K_{TM\text{-}Enc})$ containing the following information:

Certificate Information	*Value*
serialNumber	7895 CA35 014C 3D2F 1E11 B10D
Issuer	
Country Name	BE
Organisation Name	EPASOrg
Organisation Unit Name	Technical Center of Expertise
Common Name	EPAS Protocols Test CA
Validity	
notBefore	20130418101823+0100
notAfter	20181001182005+0100
Subject	
Country Name	FR
Organisation Name	EPASOrg
Organisation Unit Name	Technical Center of Expertise
Common Name	EPAS Protocol Test Host Key Encryption
Extensions	
keyUsage	KeyEncipherment

The dump of the X.509 certificate $C_{CA\text{-}TM}(K_{TM\text{-}Enc})$ is:

```
0000  30 82 05 01 30 82 02 E9 A0 03 02 01 02 02 0C 78  |0...0..........x|
0010  95 CA 35 01 4C 3D 2F 1E 11 B1 0D 30 0D 06 09 2A  |..5.L=/....0...*|
0020  86 48 86 F7 0D 01 01 0B 05 00 30 68 31 0B 30 09  |.H........0h1.0.|
0030  06 03 55 04 06 0C 02 42 45 31 10 30 0E 06 03 55  |..U....BE1.0...U|
0040  04 0A 0C 07 45 50 41 53 4F 72 67 31 26 30 24 06  |....EPASOrg1&0$.|
0050  03 55 04 0B 0C 1D 54 65 63 68 6E 69 63 61 6C 20  |.U....Technical |
0060  43 65 6E 74 65 72 20 6F 66 20 45 78 70 65 72 74  |Center of Expert|
0070  69 73 65 31 1F 30 1D 06 03 55 04 03 0C 16 45 50  |ise1.0...U....EP|
0080  41 53 20 50 72 6F 74 6F 63 6F 6C 73 20 54 65 73  |AS Protocols Tes|
0090  74 20 43 41 30 2A 18 13 32 30 31 33 30 34 31 38  |t CA0*..20130418|
00A0  31 30 31 38 32 33 2B 30 31 30 30 18 13 32 30 31  |101823+0100..201|
00B0  38 31 30 30 31 31 38 32 30 30 35 2B 30 31 30 30  |81001182005+0100|
00C0  30 78 31 0B 30 09 06 03 55 04 06 0C 02 46 52 31  |0x1.0...U....FR1|
00D0  10 30 0E 06 03 55 04 0A 0C 07 45 50 41 53 4F 72  |.0...U....EPASOr|
00E0  67 31 26 30 24 06 03 55 04 0B 0C 1D 54 65 63 68  |g1&0$..U....Tech|
00F0  6E 69 63 61 6C 20 43 65 6E 74 65 72 20 6F 66 20  |nical Center of |
0100  45 78 70 65 72 74 69 73 65 31 2F 30 2D 06 03 55  |Expertise1/0-..U|
0110  04 03 0C 26 45 50 41 53 20 50 72 6F 74 6F 63 6F  |...&EPAS Protoco|
0120  6C 20 54 65 73 74 20 48 6F 73 74 20 4B 65 79 20  |l Test Host Key |
0130  45 6E 63 72 79 70 74 69 6F 6E 30 82 01 A2 30 0D  |Encryption0...0.|
0140  06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82 01  |..*.H...........|
0150  8F 00 30 82 01 8A 02 82 01 81 00 D7 2C CF 63 FB  |..0........,.c.|
0160  2F 86 6A 18 F2 19 DC 91 93 16 49 5F F6 6C 90 6F  |/.j.......I_.l.o|
0170  90 4D 7B 26 65 25 C3 7F AB E7 D4 ED 99 EA 04 24  |.M{&e%.........$|
0180  33 6D 99 B0 B7 97 9D E1 76 4E 7C D1 6B 64 B9 BA  |3m......vN|.kd..|
0190  95 46 10 BC AC BB 6C FD A4 CB 90 6A A7 5B ED 58  |.F....l....j.[.X|
01A0  B9 A0 03 71 52 54 1E B1 DC 3D D0 B6 21 4E B3 1B  |...qRT...=..!N..|
01B0  E9 7A 4F 91 07 34 12 DE 04 22 16 FA 8F 82 6D 24  |.zO..4..."....m$|
01C0  C7 F2 D3 05 D4 BF 63 46 5B F8 99 DC 6F 07 3F F6  |......cF[...o.?.|
01D0  AA 33 8E A4 4D B6 BE 51 A6 35 8C AA 3C CB 85 28  |.3..M..Q.5..<..(|
01E0  E5 8B 55 54 0E D2 23 25 23 33 33 D3 D6 D2 B8 2E  |..UT..#%#33.....|
01F0  D7 A5 8D 49 9F 44 5F F8 35 C3 EB D5 B5 15 37 9A  |...I.D_.5.....7.|
0200  7C 2B 5B 41 D3 5F 3D FD 5A 1A 2D 61 49 10 38 FD  ||+[A._=.Z.-aI.8.|
0210  D1 9E 18 EF 67 8F D7 94 87 2A CC 8B 81 29 AF A0  |....g....*...)..|
0220  D0 2F CD 6E 4A DE 91 84 D5 FE C2 38 64 41 29 3B  |./.nJ......8dA);|
0230  16 BB 76 B8 E2 E4 F8 E8 02 76 36 68 55 A8 80 E0  |..v......v6hU...|
0240  EF AC 44 9E 76 12 4C 4B F7 FF 2B A1 5E 67 4B 62  |..D.v.LK..+.^gKb|
0250  A5 63 7D 26 60 0A A3 A0 13 E1 53 0E 11 F4 BF 98  |.c}&`.....S.....|
0260  4E 53 3F 52 0A 2E 74 BD 82 6D D5 07 C2 83 D2 F5  |NS?R..t..m......|
0270  63 C2 28 48 E0 5D 84 D2 B7 D2 22 1F 4B 63 B5 67  |c.(H.]....".Kc.g|
```

```
0280  97 E6 AF B4 25 D5 67 E5 F9 16 E3 AB 4E 2C 48 6E  |....%.g.....N,Hn|
0290  C8 14 89 46 9C 17 DA 2D FA F7 AB 49 6E E7 C2 4E  |...F...-...In..N|
02A0  43 95 1F FE 28 00 6B FF 96 E2 D1 58 38 AC 72 52  |C...(.k....X8.rR|
02B0  F3 D4 5E 8F EB EF 0F 7E EF 97 4F FE 0A 38 C3 89  |..^....~..O..8..|
02C0  26 CF A0 68 31 98 CA 8F D0 8C 8B 24 27 B9 1A 0B  |&..h1......$'...|
02D0  16 F7 9A 71 86 DE 7D AB 9D FF 3D 02 03 01 00 01  |...q..}...=.....|
02E0  A3 0F 30 0D 30 0B 06 03 55 1D 0F 04 04 03 02 05  |..0.0...U.......|
02F0  20 30 0D 06 09 2A 86 48 86 F7 0D 01 01 0B 05 00  | 0...*.H........|
0300  03 82 02 01 00 26 ED 5F 4E 11 5A 9E 2D 10 F0 7B  |.....&._N.Z.-..{|
0310  35 D1 0F 35 D8 BD 3B B4 0D 48 1E 5F 0D 2E 08 C8  |5..5..;..H._....|
0320  02 41 D7 00 02 BA 5C 73 07 49 1C E2 89 53 CB 70  |.A....\s.I...S.p|
0330  D4 9D 85 D2 0D 0B BA FD BD C4 04 EF B7 AE DD 2B  |...............+|
0340  5E 92 92 EA 76 84 78 3E 02 DC 98 95 5C FB 1D 94  |^...v.x>....\...|
0350  17 19 E1 E4 8F F8 3F 11 74 10 24 35 B3 52 59 E7  |......?.t.$5.RY.|
0360  50 9F 8F B6 7C 30 DD BE E7 B5 F5 40 AD 89 00 35  |P...|0.....@...5|
0370  D6 04 B9 8D 2F 08 14 E7 8F 8F 9D E9 D4 B7 7A F7  |..../.........z.|
0380  26 DB 66 7C CA F7 0A 17 5A F8 7F 71 69 79 CA 87  |&.f|....Z..qiy..|
0390  83 A8 24 7E 3C F3 6B D8 DC 31 6F E1 D6 31 A2 48  |..$~<.k..1o..1.H|
03A0  96 25 3D 12 42 AE 65 9E 3E A1 5A 82 E7 3C 4B 29  |.%=.B.e.>.Z..<K)|
03B0  64 57 AF 5F 08 8B 00 F6 EF 51 73 0E E5 E4 FA 9B  |dW._.....Qs.....|
03C0  AF 6E D8 E4 CC 34 F0 FB 90 FF 44 42 D4 55 F3 61  |.n...4....DB.U.a|
03D0  9A 50 59 CA 82 DD 15 CB 40 13 02 E7 0F 12 4B DE  |.PY.....@.....K.|
03E0  6D 51 41 56 FB 42 DD E6 AD A6 20 EF 2D 27 B7 F2  |mQAV.B.... .-'..|
03F0  18 9B 4F CA B9 F4 48 7D A2 6E D4 41 8F 00 EA 4C  |..O...H}.n.A...L|
0400  7A 89 30 8E AC 88 E5 86 59 43 F9 5F 08 7A 6F B7  |z.0.....YC._.zo.|
0410  74 9B DB 78 3E 2A E2 8F F7 C4 10 AD C9 35 F4 16  |t..x>*.......5..|
0420  58 F3 6C D9 0F 2C C8 95 A2 7D B5 AD 1E F1 47 AA  |X.l..,...}....G.|
0430  60 63 4A 65 91 C3 43 AC 7F F9 5C 6D 7D 7C B8 8E  |`cJe..C...\m}|..|
0440  BB 36 16 91 FD A5 86 55 1D 6F 0C AD 7F E5 F0 37  |.6.....U.o.....7|
0450  46 03 50 E5 D0 A6 50 D6 27 EB 0C 1B 53 15 B0 49  |F.P...P.'...S..I|
0460  24 14 68 42 30 BB A2 39 D5 CA B9 89 42 07 9D AB  |$.hB0..9....B...|
0470  4F 0C BB CE B2 D8 81 D0 FF E8 B2 E1 9D B8 F9 4A  |O..............J|
0480  E9 D9 9B AC 6B E2 C4 8E 5F E4 5D EE C2 FF E8 FA  |....k..._.].....|
0490  F5 2B 43 25 6B C5 0E 17 F0 CE F1 AB 8B 86 94 FC  |.+C%k...........|
04A0  34 93 62 7C F2 85 22 83 B2 51 76 DD AF EE 8F BA  |4.b|.."..Qv.....|
04B0  49 F4 34 D2 B7 F1 BC AF 79 CC B3 EA D1 5F 3A 6D  |I.4.....y...._:m|
04C0  11 93 9E DC 40 63 52 DF 6A 68 F1 20 18 31 CE D0  |....@cR.jh. .1..|
04D0  FE 20 5E 1F 38 15 F4 6E 01 E6 E5 F5 79 8D E2 EF  |. ^.8..n....y...|
04E0  B7 CF 6E FE 57 8B A3 3A ED BB 3E D9 C4 EF 39 EA  |..n.W..:..>...9.|
04F0  5E 9A 68 99 CE 00 DB 6C 89 22 45 0A A1 82 27 54  |^.h....l."E...'T|
0500  9D B4 3F 16 43                                   |..?.C           |
```

1.4.3 Initial Status of the Keys

The POI contact the key injection server, sending the *StatusReport* message containing the header and the body presented in the table below:

Message Item	*Value*
Header	
DownloadTransfer	False
FormatVersion	6.0
ExchangeIdentification	001
CreationDateTime	2013-12-06:13:53:49.00+02:00
InitiatingParty	
Identification	66000001
Type	OriginatingPOI
Issuer	MasterTerminalManager
RecipientParty	
Identification	epas-keyDownload-TM1
Type	MasterTerminalManager
StatusReport	
POIIdentification	
Identification	66000001
Type	OriginationgPOI
Issuer	MasterTerminalManager
TerminalManagerdentification	
Identification	epas-keyDownload-TM1
Type	MasterTerminalManager
DataSet	
Identification	
Type	StatusReport
CreationDateTime	2013-12-06:13:53:49.00+02:00
Content	
POIComponent	
Type	Terminal
Identification	
ItemNumber	1
ProviderIdentification	EPASVendor001
Identification	Counter Top E41
SerialNumber	7825410759
POIComponent	
Type	PaymentApplication
Identification	
ItemNumber	1.1
ProviderIdentification	EPASVendor001
Status	
VersionNumber	1.01
StandardCompliance	
Identification	SEPA-FAST
VersionNumber	3.0
Issuer	CIR
AttendanceContext	Attended
POIDateTime	2013-12-06:13:53:49.00+02:00

The POI has no symmetric key shared usable by the key injection, so the pre-loaded authentication RSA key is used to provide a digital signature of the message body.

Once unnecessary spaces and carriage returns are removed, the XML encoded *StatusReport* message body is:

```
0000  3C 53 74 73 52 70 74 3E 3C 50 4F 49 49 64 3E 3C  |<StsRpt><POIId><|
0010  49 64 3E 36 36 30 30 30 30 30 31 3C 2F 49 64 3E  |Id>66000001</Id>|
0020  3C 54 70 3E 4F 50 4F 49 3C 2F 54 70 3E 3C 49 73  |<Tp>OPOI</Tp><Is|
0030  73 72 3E 4D 54 4D 47 3C 2F 49 73 73 72 3E 3C 2F  |sr>MTMG</Issr></|
0040  50 4F 49 49 64 3E 3C 54 65 72 6D 6E 6C 4D 67 72  |POIId><TermnlMgr|
0050  49 64 3E 3C 49 64 3E 65 70 61 73 2D 6B 65 79 44  |Id><Id>epas-keyD|
0060  6F 77 6E 6C 6F 61 64 2D 54 4D 31 3C 2F 49 64 3E  |ownload-TM1</Id>|
0070  3C 54 70 3E 4D 54 4D 47 3C 2F 54 70 3E 3C 2F 54  |<Tp>MTMG</Tp></T|
0080  65 72 6D 6E 6C 4D 67 72 49 64 3E 3C 44 61 74 61  |ermnlMgrId><Data|
0090  53 65 74 3E 3C 49 64 3E 3C 54 70 3E 53 54 52 50  |Set><Id><Tp>STRP|
00A0  3C 2F 54 70 3E 3C 43 72 65 44 74 54 6D 3E 32 30  |</Tp><CreDtTm>20|
00B0  31 33 2D 31 32 2D 30 36 54 31 33 3A 35 33 3A 34  |13-12-06T13:53:4|
00C0  39 2E 30 30 2B 30 32 3A 30 30 3C 2F 43 72 65 44  |9.00+02:00</CreD|
00D0  74 54 6D 3E 3C 2F 49 64 3E 3C 43 6E 74 74 3E 3C  |tTm></Id><Cntt><|
00E0  50 4F 49 43 6D 70 6E 74 3E 3C 54 70 3E 54 45 52  |POICmpnt><Tp>TER|
00F0  4D 3C 2F 54 70 3E 3C 49 64 3E 3C 49 74 6D 4E 62  |M</Tp><Id><ItmNb|
0100  3E 31 3C 2F 49 74 6D 4E 62 3E 3C 50 72 76 64 72  |>1</ItmNb><Prvdr|
0110  49 64 3E 45 50 41 53 56 65 6E 64 6F 72 30 30 31  |Id>EPASVendor001|
0120  3C 2F 50 72 76 64 72 49 64 3E 3C 49 64 3E 43 6F  |</PrvdrId><Id>Co|
0130  75 6E 74 65 72 20 54 6F 70 20 45 34 31 3C 2F 49  |unter Top E41</I|
0140  64 3E 3C 53 72 6C 4E 62 3E 37 38 32 35 34 31 30  |d><SrlNb>7825410|
0150  37 35 39 3C 2F 53 72 6C 4E 62 3E 3C 2F 49 64 3E  |759</SrlNb></Id>|
0160  3C 2F 50 4F 49 43 6D 70 6E 74 3E 3C 50 4F 49 43  |</POICmpnt><POIC|
0170  6D 70 6E 74 3E 3C 54 70 3E 41 50 4C 49 3C 2F 54  |mpnt><Tp>APLI</T|
0180  70 3E 3C 49 64 3E 3C 49 74 6D 4E 62 3E 31 2E 31  |p><Id><ItmNb>1.1|
0190  3C 2F 49 74 6D 4E 62 3E 3C 50 72 76 64 72 49 64  |</ItmNb><PrvdrId|
01A0  3E 45 50 41 53 56 65 6E 64 6F 72 30 30 31 3C 2F  |>EPASVendor001</|
01B0  50 72 76 64 72 49 64 3E 3C 2F 49 64 3E 3C 53 74  |PrvdrId></Id><St|
01C0  73 3E 3C 56 72 73 6E 4E 62 3E 31 2E 30 31 3C 2F  |s><VrsnNb>1.01</|
01D0  56 72 73 6E 4E 62 3E 3C 2F 53 74 73 3E 3C 53 74  |VrsnNb></Sts><St|
01E0  64 43 6D 70 6C 63 3E 3C 49 64 3E 53 45 50 41 2D  |dCmplc><Id>SEPA-|
01F0  46 41 53 54 3C 2F 49 64 3E 3C 56 72 73 6E 3E 33  |FAST</Id><Vrsn>3|
0200  2E 30 3C 2F 56 72 73 6E 3E 3C 49 73 73 72 3E 43  |.0</Vrsn><Issr>C|
0210  49 52 3C 2F 49 73 73 72 3E 3C 2F 53 74 64 43 6D  |IR</Issr></StdCm|
0220  70 6C 63 3E 3C 2F 50 4F 49 43 6D 70 6E 74 3E 3C  |plc></POICmpnt><|
0230  41 74 74 6E 64 6E 63 43 6E 74 78 74 3E 41 54 54  |AttndncCntxt>ATT|
0240  44 3C 2F 41 74 74 6E 64 6E 63 43 6E 74 78 74 3E  |D</AttndncCntxt>|
0250  3C 50 4F 49 44 74 54 6D 3E 32 30 31 33 2D 31 32  |<POIDtTm>2013-12|
0260  2D 30 36 54 31 33 3A 35 33 3A 34 39 2E 30 30 2B  |-06T13:53:49.00+|
0270  30 32 3A 30 30 3C 2F 50 4F 49 44 74 54 6D 3E 3C  |02:00</POIDtTm><|
0280  2F 43 6E 74 74 3E 3C 2F 44 61 74 61 53 65 74 3E  |/Cntt></DataSet>|
0290  3C 2F 53 74 73 52 70 74 3E                      |</StsRpt>       |
```

The SHA256 digest of the *StatusReport* message body is:

```
0000  A1 1B 8D 78 72 94 2C 4A C5 9E 7C A8 41 5F A2 9F  |...xr.,J..|.A_..|
0010  05 15 24 81 26 DB D1 47 62 AF B5 EE 7E B1 B2 5E  |..$.&..Gb...~..^|
```

Applying the padding process for the digital signature, the block result is dumped below:

```
0000  00 01 FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0010  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0020  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0030  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0040  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0050  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0060  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0070  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0080  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0090  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
00A0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
00B0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
00C0  FF FF FF FF FF FF FF FF FF FF FF FF 00 30 31 30  |.............010|
00D0  0D 06 09 60 86 48 01 65 03 04 02 01 05 00 04 20  |...`.H.e....... |
00E0  A1 1B 8D 78 72 94 2C 4A C5 9E 7C A8 41 5F A2 9F  |...xr.,J..|.A_..|
00F0  05 15 24 81 26 DB D1 47 62 AF B5 EE 7E B1 B2 5E  |..$.&..Gb...~..^|
```

After encryption by the private key of $K_{POI\text{-}Sign}$, we have the digital signature of the *StatusReport* message body:

```
0000  6E 0E 57 07 DF E9 8A 0A F8 D5 7D B7 55 60 12 5C  |n.W.......}.U`.\|
0010  49 7A 90 98 4F E7 4E 06 A2 54 20 1A B6 F6 A9 C5  |Iz..O.N..T .....|
0020  0D 04 C2 9D EB FA 16 D1 55 51 E3 73 1B 70 1D C3  |........UQ.s.p..|
0030  CA 3C 7D CA 37 13 2F C5 B0 B3 7D 49 32 BE 13 10  |.<}.7./...}I2...|
0040  CE 79 CF 0D 2F A8 4A D7 6D B8 7D 05 FC 02 70 63  |.y../.J.m.}...pc|
0050  B2 4D FE A1 88 92 A5 02 1C E5 3D 24 E6 86 D8 56  |.M........=$...V|
0060  45 B7 74 3F E4 A8 2D 15 CA AD DD 72 5C AD 38 1E  |E.t?..-....r\.8.|
0070  C7 A1 AD E7 A7 A7 DB 83 79 5C BD F4 41 3D C3 AD  |........y\..A=..|
0080  A4 D6 65 C8 9B AD 9A D9 EE 68 A1 08 00 27 5F 9F  |..e......h...'_.|
0090  D0 4E 4D C1 F0 1B B1 5C EE 02 A0 7F F0 5A FE 8E  |.NM....\.....Z..|
00A0  3E 71 F3 E7 30 40 0A 56 41 D1 72 95 2D A0 72 8E  |>q..0@.VA.r.-.r.|
00B0  D6 73 D4 51 A6 0D 97 FF FD AF A0 52 18 5E 84 43  |.s.Q.......R.^.C|
00C0  8D 24 FE D3 29 3D AF 64 25 43 E0 E6 3C 2D DE D0  |.$..)=.d%C..<-..|
00D0  DA 6A 10 65 A0 D3 A2 8A F9 04 48 6A 90 BF 43 D2  |.j.e......Hj..C.|
00E0  AA 23 58 0D D2 FA 39 16 CB 59 39 4A 40 E4 55 9A  |.#X...9..Y9J@.U.|
00F0  D9 FE EE 08 45 00 D0 C6 E0 41 DF BA 24 F2 07 19  |....E....A..$...|
```

748 Inside the *SecurityTrailer*, the *SignedData* CMS data structure is presented in the table below:

Message Item	*Value*
SecurityTrailer	
SignedData	
ContentType	SignedData
DigestAlgorithm	
Algorithm	SHA256
EncapsulatedContent	
ContentType	PlainData
Certificate	308204833082026BA003020102020C2225A8FB00071293D4641C3C300D06092A 864886F70D01010B05003068310B300906035504060C0242453110300E060355 040A0C07455041534F72673126302406035504 0B0C1D546563686E6963616C20 43656E746572206F662045787065727469736531 1F301D06035504030C164550 41532050726F746F636F6C732054657374204341302A181332303133303431 38 3130323534362B303130301813323031383130303131383230303052B30313030 307A310B300906035504060C0246523110300E060355040A0C07455041534F72 673126302406035504 0B0C1D546563686E6963616C2043656E746572206F6620 45787065727469736531 31302F06035504030C28455041532050726F746F636F 6C205465737420436C69656E742041757468656E7469636174696F6E30820122 300D06092A864886F70D01010105000382010F003082010A0282010100C22511 390B85DB3990A27638B850616C18B11BDF78494B48B61F8F8D032225A8FB0007 1293D4641C3CDDE18D47337EB7381AC12976820FF5C0B321E4EDF88C9B8F1627 0E0FC6FAB470449BA70B947139551ABE326686F538C4F7F63A45FF4CB9E66470 00B28B791E1205ADB6ACDC29854698D90ACC3B6C84F0F8C2EFBEE4E3F9844BD7 9AB14C1F22376198C13BEAC560DDC835104176729C7E62FBF4EC350DE4D385C4 8D3EA40A90D7AA5838FAED3E3C760D19BB84D1997077C72331F3ADF050B41DB5 FFD19D129E88C75331DA13264BE4C2F0B0A0AA09F77EED2C801FAD239E8FE5D8 B43F10708FC3D6054B9156C5B55184F1A294DAB8F8267162BE9BB54867020301 0001A30F300D300B0603551D0F040403020780300D06092A864886F70D01010B 05000382020100540DB4CCCA78C5B72EC34D6A55EE7C152ED54409419E0B7BC7 83B8559557C02CCA5E81B6CCA854A36250ADCA0CD55C96F42F019799B5A100C9 72D3F2411CB2676300F1B09E46AE4F293A24CB71EEA5467CB91933713E556FFC C0B558DA344FF4F8AB30A2F803BD97BB568100BAC6B6FAE884F831BF855C4EE8 23FE3BAC3BA2D8B615F62C1C1685B9BC59DFCBE1CFBDFDB29F3773FD46685688 BF656670F5BB9CE56B029E36E7291629DE69FA858367619D8DE4FB9F08608518 85A42894ADC97DCB51D4CEBF9F52083DD511371B157E3D16F93469EED0B7FF01 BC137D5065E266A8EA3C82999EF36263A863ED5FE22A69E4874FDF41A19FA457 B12CF6A52B08F73BD3BD9C2FD13352ECEE4EEF6323826BF72440FC149EBD5891 A8D6D0E5DA50547708525CA4021B51059B52B50E61B176C1F962AA7AC2809934 31DD5BF3D6C146ADBA762B3E6729F17FA639D98D5CBFDCAE556A2FC0B23754E4 91F97BF17A18D842A87F8DE4FBA58B56517213BC59C512D4F0447F0C197B3878 5A457E0A0E7DD44806C4BA16F811B7A25024791ED742E74392C9D4BABA754F09 B61DD8EC2ABBF6737E492BBC37185072AC9EBEA3DEF2FBD56E836B88D0809F96 A4B2ACA1A5B59D198F94990BA4D2A1B50CF64C5E8391D6DCADB58C9E074E608D 7D012309A92FFDCEFD96CDAEA4F6BE5E572A20161C3D6FD838FFAE966BB2C671 E7C836FB369C28
Signer	
SignerIdentification	
IssuerAnd-SerialNumber	
Issuer	
RelativeDistin-guishedName	
AttributeType	CountryName
AttributeValue	BE
RelativeDistin-guishedName	
AttributeType	OrganisationName
AttributeValue	EPASOrg
RelativeDistin-guishedName	
AttributeType	OrganisationUnitName
AttributeValue	Technical Center of Expertise

RelativeDistinguishedName	
AttributeType	CommonName
AttributeValue	EPAS Protocols Test CA
SerialNumber	2225A8FB00071293D4641C3C
DigestAlgorithm	
Algorithm	SHA256
SignatureAlgorithm	
Algorithm	SHA256WithRSA
Signature	6E0E5707DFE98A0AF8D57DB75560125C497A90984FE74E06A254201AB6F6A9C5 0D04C29DEBFA16D15551E3731B701DC3CA3C7DCA37132FC5B0B37D4932BE1310 CE79CF0D2FA84AD76DB87D05FC027063B24DFEA18892A5021CE53D24E686D856 45B7743FE4A82D15CAADDD725CAD381EC7A1ADE7A7A7DB83795CBDF4413DC3AD A4D665C89BAD9AD9EE68A10800275F9FD04E4DC1F01BB15CEE02A07FF05AFE8E 3E71F3E730400A5641D172952DA0728ED673D451A60D97FFFDAFA052185E8443 8D24FED3293DAF642543E0E63C2DDED0DA6A1065A0D3A28AF904486A90BF43D2 AA23580DD2FA3916CB59394A40E4559AD9FEEE084500D0C6E041DFBA24F20719

The XML encoded structure of the *StatusReport* message is:

```
<?xml version="1.0" encoding="UTF-8"?>
<Document xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="urn:iso:std:iso:20022:tech:xsd:catm.001.001.06">
 <StsRpt>
    <Hdr>
       <DwnldTrf>false</DwnldTrf>
       <FrmtVrsn>6.0</FrmtVrsn>
       <XchgId>001</XchgId>
       <CreDtTm>2013-12-06T13:53:49.00+02:00</CreDtTm>
       <InitgPty>
          <Id>66000001</Id>
          <Tp>OPOI</Tp>
          <Issr>MTMG</Issr>
       </InitgPty>
       <RcptPty>
          <Id>epas-keyDownload-TM1</Id>
          <Tp>MTMG</Tp>
       </RcptPty>
    </Hdr>
    <StsRpt>
       <POIId>
          <Id>66000001</Id>
          <Tp>OPOI</Tp>
          <Issr>MTMG</Issr>
       </POIId>
       <TermnlMgrId>
          <Id>epas-keyDownload-TM1</Id>
          <Tp>MTMG</Tp>
       </TermnlMgrId>
       <DataSet>
          <Id>
             <Tp>STRP</Tp>
             <CreDtTm>2013-12-06T13:53:49.00+02:00</CreDtTm>
          </Id>
          <Cntt>
             <POICmpnt>
                <Tp>TERM</Tp>
                <Id>
                   <ItmNb>1</ItmNb>
                   <PrvdrId>EPASVendor001</PrvdrId>
                   <Id>Counter Top E41</Id>
                   <SrlNb>7825410759</SrlNb>
                </Id>
             </POICmpnt>
             <POICmpnt>
```

```
            <Tp>APLI</Tp>
            <Id>
               <ItmNb>1.1</ItmNb>
               <PrvdrId>EPASVendor001</PrvdrId>
            </Id>
            <Sts>
               <VrsnNb>1.01</VrsnNb>
            </Sts>
            <StdCmplc>
               <Id>SEPA-FAST</Id>
               <Vrsn>3.0</Vrsn>
               <Issr>CIR</Issr>
            </StdCmplc>
         </POICmpnt>
         <AttndncCntxt>ATTD</AttndncCntxt>
         <POIDtTm>2013-12-06T13:53:49.00+02:00</POIDtTm>
      </Cntt>
   </DataSet>
</StsRpt>
<SctyTrlr>
   <CnttTp>SIGN</CnttTp>
   <SgndData>
      <DgstAlgo>
         <Algo>HS25</Algo>
      </DgstAlgo>
      <NcpsltdCntt>
         <CnttTp>DATA</CnttTp>
      </NcpsltdCntt>
      <Cert>
         MIIEgzCCAmugAwIBAgIMIiWo+wAHEpPUZBw8MA0GCSqGSIb3DQEBCwUAMGgxCzAJBgNVBAYMAkJFMR
         AwDgYDVQQKDAdFUEFTT3JnMSYwJAYDVQQLDB1UZWNobmljYWwgQ2VudGVyIG9mIEV4cGVydGlzZTEf
         MB0GA1UEAwwWRVBBUyBQcm90b2NvbHMgVGVzdCBDQTAqGBMyMDEzMDQxODEwMjU0NiswMTAwGBMyMD
         E4MTAwMTE4MjAwNSswMTAwMHoxCzAJBgNVBAYMAkZSMRAwDgYDVQQKDAdFUEFTT3JnMSYwJAYDVQQL
         DB1UZWNobmljYWwgQ2VudGVyIG9mIEV4cGVydGlzZTExMC8GA1UEAwwoRVBBUyBQcm90b2NvbCBUZX
         N0IENsaWVudCBBdXRoZW50aWNhdGlvbjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMIl
         ETkLhds5kKJ2OLhQYWwYsRvfeElLSLYfj40DIiWo+wAHEpPUZBw83eGNRzN+tzgawSl2gg/1wLMh5O
         34jJuPFicOD8b6tHBEm6cLlHE5VRq+MmaG9TjE9/Y6Rf9MueZkcACyi3keEgWttqzcKYVGmNkKzDts
         hPD4wu++5OP5hEvXmrFMHyI3YZjBO+rFYN3INRBBdnKcfmL79Ow1DeTThcSNPqQKkNeqWDj67T48dg
         0Zu4TRmXB3xyMx863wULQdtf/RnRKeiMdTMdoTJkvkwvCwoKoJ937tLIAfrSOej+XYtD8QcI/D1gVL
         kVbFtVGE8aKU2rj4JnFivpu1SGcCAwEAAaMPMA0wCwYDVR0PBAQDAgeAMA0GCSqGSIb3DQEBCwUAA4
         ICAQBUDbTMynjFty7DTWpV7nwVLtVECUGeC3vHg7hVlVfALMpegbbMqFSjYlCtygzVXJb0LwGXmbWh
         AMly0/JBHLJnYwDxsJ5Grk8pOiTLce6lRny5GTNxPlVv/MC1WNo0T/T4qzCi+AO9l7tWgQC6xrb66I
         T4Mb+FXE7oI/47rDui2LYV9iwcFoW5vFnfy+HPvf2ynzdz/UZoVoi/ZWZw9buc5WsCnjbnKRYp3mn6
         hYNnYZ2N5PufCGCFGIWkKJStyX3LUdTOv59SCD3VETcbFX49Fvk0ae7Qt/8BvBN9UGXiZqjqPIKZnv
         NiY6hj7V/iKmnkh0/fQaGfpFexLPalKwj3O9O9nC/RM1Ls7k7vYyOCa/ckQPwUnr1YkajW0OXaUFR3
         CFJcpAIbUQWbUrUOYbF2wfliqnrCgJk0Md1b89bBRq26dis+Zynxf6Y52Y1cv9yuVWovwLI3VOSR+X
         vxehjYQqh/jeT7pYtWUXITvFnFEtTwRH8MGXs4eFpFfgoOfdRIBsS6FvgRt6JQJHke10LnQ5LJ1Lq6
         dU8Jth3Y7Cq79nN+SSu8NxhQcqyevqPe8vvVboNriNCAn5aksqyhpbWdGY+UmQuk0qG1DPZMXoOR1t
         yttYyeB05gjX0BIwmpL/3O/ZbNrqT2vl5XKiAWHD1v2Dj/rpZrssZx58g2+zacKA==
      </Cert>
      <Sgnr>
         <SgnrId>
            <IssrAndSrlNb>
               <Issr>
                  <RltvDstngshdNm>
                        <AttrTp>CATT</AttrTp>
                        <AttrVal>BE</AttrVal>
                  </RltvDstngshdNm>
                  <RltvDstngshdNm>
                        <AttrTp>OATT</AttrTp>
                        <AttrVal>EPASOrg</AttrVal>
                  </RltvDstngshdNm>
                  <RltvDstngshdNm>
                        <AttrTp>OUAT</AttrTp>
                        <AttrVal>Technical Center of Expertise</AttrVal>
                  </RltvDstngshdNm>
                  <RltvDstngshdNm>
                        <AttrTp>CNAT</AttrTp>
                        <AttrVal>EPAS Protocols Test CA</AttrVal>
```

```
                  </RltvDstngshdNm>
               </Issr>
               <SrlNb>IiWo+wAHEpPUZBw8</SrlNb>
            </IssrAndSrlNb>
         </SgnrId>
            <DgstAlgo>
               <Algo>HS25</Algo>
            </DgstAlgo>
            <SgntrAlgo>
               <Algo>ERS2</Algo>
            </SgntrAlgo>
            <Sgntr>
               bg5XB9/pigr41X23VWASXEl6kJhP504GolQgGrb2qcUNBMKd6/oW0VVR43MbcB3Dyjx9yjcTL
               8Wws31JMr4TEM55zw0vqErXbbh9BfwCcGOyTf6hiJKlAhzlPSTmhthWRbd0P+SoLRXKrd1yXK
               04Hsehreenp9uDeVy99EE9w62k1mXIm62a2e5ooQgAJ1+f0E5NwfAbsVzuAqB/8Fr+jj5x8+c
               wQApWQdFylS2gco7Wc9RRpg2X//2voFIYXoRDjST+0yk9r2QlQ+DmPC3e0NpqEGWg06KK+QRI
               apC/Q9KqI1gN0vo5FstZOUpA5FWa2f7uCEUA0MbgQd+6JPIHGQ==

            </Sgntr>
       </Sgnr>
    </SgndData>
 </SctyTrlr>
</StsRpt>
</Document>
```

Once unnecessary spaces and carriage returns are removed, the XML encoded *SecurityTrailer* structure is:

```
0000  3C 53 63 74 79 54 72 6C 72 3E 3C 43 6E 74 74 54  |<SctyTrlr><CnttT|
0010  70 3E 53 49 47 4E 3C 2F 43 6E 74 74 54 70 3E 3C  |p>SIGN</CnttTp><|
0020  53 67 6E 64 44 61 74 61 3E 3C 44 67 73 74 41 6C  |SgndData><DgstAl|
0030  67 6F 3E 3C 41 6C 67 6F 3E 48 53 32 35 3C 2F 41  |go><Algo>HS25</A|
0040  6C 67 6F 3E 3C 2F 44 67 73 74 41 6C 67 6F 3E 3C  |lgo></DgstAlgo><|
0050  4E 63 70 73 6C 74 64 43 6E 74 74 3E 3C 43 6E 74  |NcpsltdCntt><Cnt|
0060  74 54 70 3E 44 41 54 41 3C 2F 43 6E 74 74 54 70  |tTp>DATA</CnttTp|
0070  3E 3C 2F 4E 63 70 73 6C 74 64 43 6E 74 74 3E 3C  |></NcpsltdCntt><|
0080  43 65 72 74 3E 4D 49 49 45 67 7A 43 43 41 6D 75  |Cert>MIIEgzCCAmu|
0090  67 41 77 49 42 41 67 49 4D 49 69 57 6F 2B 77 41  |gAwIBAgIMIiWo+wA|
00A0  48 45 70 50 55 5A 42 77 38 4D 41 30 47 43 53 71  |HEpPUZBw8MA0GCSq|
00B0  47 53 49 62 33 44 51 45 42 43 77 55 41 4D 47 67  |GSIb3DQEBCwUAMGg|
00C0  78 43 7A 41 4A 42 67 4E 56 42 41 59 4D 41 6B 4A  |xCzAJBgNVBAYMAkJ|
00D0  46 4D 52 41 77 44 67 59 44 56 51 51 4B 44 41 64  |FMRAwDgYDVQQKDAd|
00E0  46 55 45 46 54 54 33 4A 6E 4D 53 59 77 4A 41 59  |FUEFTT3JnMSYwJAY|
00F0  44 56 51 51 4C 44 42 31 55 5A 57 4E 6F 62 6D 6C  |DVQQLDB1UZWNobml|
0100  6A 59 57 77 67 51 32 56 75 64 47 56 79 49 47 39  |jYWwgQ2VudGVyIG9|
0110  6D 49 45 56 34 63 47 56 79 64 47 6C 7A 5A 54 45  |mIEV4cGVydGlzZTE|
0120  66 4D 42 30 47 41 31 55 45 41 77 77 57 52 56 42  |fMB0GA1UEAwwWRVB|
0130  42 55 79 42 51 63 6D 39 30 62 32 4E 76 62 48 4D  |BUyBQcm90b2NvbHM|
0140  67 56 47 56 7A 64 43 42 44 51 54 41 71 47 42 4D  |gVGVzdCBDQTAqGBM|
0150  79 4D 44 45 7A 4D 44 51 78 4F 44 45 77 4D 6A 55  |yMDEzMDQxODEwMjU|
0160  30 4E 69 73 77 4D 54 41 77 47 42 4D 79 4D 44 45  |0NiswMTAwGBMyMDE|
0170  34 4D 54 41 77 4D 54 45 34 4D 6A 41 77 4E 53 73  |4MTAwMTE4MjAwNSs|
0180  77 4D 54 41 77 4D 48 6F 78 43 7A 41 4A 42 67 4E  |wMTAwMHoxCzAJBgN|
0190  56 42 41 59 4D 41 6B 5A 53 4D 52 41 77 44 67 59  |VBAYMAkZSMRAwDgY|
01A0  44 56 51 51 4B 44 41 64 46 55 45 46 54 54 33 4A  |DVQQKDAdFUEFTT3J|
01B0  6E 4D 53 59 77 4A 41 59 44 56 51 51 4C 44 42 31  |nMSYwJAYDVQQLDB1|
01C0  55 5A 57 4E 6F 62 6D 6C 6A 59 57 77 67 51 32 56  |UZWNobmljYWwgQ2V|
01D0  75 64 47 56 79 49 47 39 6D 49 45 56 34 63 47 56  |udGVyIG9mIEV4cGV|
01E0  79 64 47 6C 7A 5A 54 45 78 4D 43 38 47 41 31 55  |ydGlzZTExMC8GA1U|
01F0  45 41 77 77 6F 52 56 42 42 55 79 42 51 63 6D 39  |EAwwoRVBBUyBQcm9|
0200  30 62 32 4E 76 62 43 42 55 5A 58 4E 30 49 45 4E  |0b2NvbCBUZXN0IEN|
0210  73 61 57 56 75 64 43 42 42 64 58 52 6F 5A 57 35  |saWVudCBBdXRoZW5|
0220  30 61 57 4E 68 64 47 6C 76 62 6A 43 43 41 53 49  |0aWNhdGlvbjCCASI|
0230  77 44 51 59 4A 4B 6F 5A 49 68 76 63 4E 41 51 45  |wDQYJKoZIhvcNAQE|
0240  42 42 51 41 44 67 67 45 50 41 44 43 43 41 51 6F  |BBQADggEPADCCAQo|
0250  43 67 67 45 42 41 4D 49 6C 45 54 6B 4C 68 64 73  |CggEBAMIlETkLhds|
0260  35 6B 4B 4A 32 4F 4C 68 51 59 57 77 59 73 52 76  |5kKJ2OLhQYWwYsRv|
0270  66 65 45 6C 4C 53 4C 59 66 6A 34 30 44 49 69 57  |feElLSLYfj40DIiW|
0280  6F 2B 77 41 48 45 70 50 55 5A 42 77 38 33 65 47  |o+wAHEpPUZBw83eG|
0290  4E 52 7A 4E 2B 74 7A 67 61 77 53 6C 32 67 67 2F  |NRzN+tzgawSl2gg/|
02A0  31 77 4C 4D 68 35 4F 33 34 6A 4A 75 50 46 69 63  |1wLMh5O34jJuPFic|
02B0  4F 44 38 62 36 74 48 42 45 6D 36 63 4C 6C 48 45  |OD8b6tHBEm6cLlHE|
02C0  35 56 52 71 2B 4D 6D 61 47 39 54 6A 45 39 2F 59  |5VRq+MmaG9TjE9/Y|
02D0  36 52 66 39 4D 75 65 5A 6B 63 41 43 79 69 33 6B  |6Rf9MueZkcACyi3k|
02E0  65 45 67 57 74 74 71 7A 63 4B 59 56 47 6D 4E 6B  |eEgWttqzcKYVGmNk|
02F0  4B 7A 44 74 73 68 50 44 34 77 75 2B 2B 35 4F 50  |KzDtshPD4wu++5OP|
0300  35 68 45 76 58 6D 72 46 4D 48 79 49 33 59 5A 6A  |5hEvXmrFMHyI3YZj|
0310  42 4F 2B 72 46 59 4E 33 49 4E 52 42 42 64 6E 4B  |BO+rFYN3INRBBdnK|
0320  63 66 6D 4C 37 39 4F 77 31 44 65 54 54 68 63 53  |cfmL79Ow1DeTThcS|
0330  4E 50 71 51 4B 6B 4E 65 71 57 44 6A 36 37 54 34  |NPqQKkNeqWDj67T4|
0340  38 64 67 30 5A 75 34 54 52 6D 58 42 33 78 79 4D  |8dg0Zu4TRmXB3xyM|
0350  78 38 36 33 77 55 4C 51 64 74 66 2F 52 6E 52 4B  |x863wULQdtf/RnRK|
0360  65 69 4D 64 54 4D 64 6F 54 4A 6B 76 6B 77 76 43  |eiMdTMdoTJkvkwvC|
0370  77 6F 4B 6F 4A 39 33 37 74 4C 49 41 66 72 53 4F  |woKoJ937tLIAfrSO|
0380  65 6A 2B 58 59 74 44 38 51 63 49 2F 44 31 67 56  |ej+XYtD8QcI/D1gV|
0390  4C 6B 56 62 46 74 56 47 45 38 61 4B 55 32 72 6A  |LkVbFtVGE8aKU2rj|
03A0  34 4A 6E 46 69 76 70 75 31 53 47 63 43 41 77 45  |4JnFivpu1SGcCAwE|
03B0  41 41 61 4D 50 4D 41 30 77 43 77 59 44 56 52 30  |AAaMPMA0wCwYDVR0|
03C0  50 42 41 51 44 41 67 65 41 4D 41 30 47 43 53 71  |PBAQDAgeAMA0GCSq|
03D0  47 53 49 62 33 44 51 45 42 43 77 55 41 41 34 49  |GSIb3DQEBCwUAA4I|
03E0  43 41 51 42 55 44 62 54 4D 79 6E 6A 46 74 79 37  |CAQBUDbTMynjFty7|
03F0  44 54 57 70 56 37 6E 77 56 4C 74 56 45 43 55 47  |DTWpV7nwVLtVECUG|
0400  65 43 33 76 48 67 37 68 56 6C 56 66 41 4C 4D 70  |eC3vHg7hVlVfALMp|
0410  65 67 62 62 4D 71 46 53 6A 59 6C 43 74 79 67 7A  |egbbMqFSjYlCtygz|
0420  56 58 4A 62 30 4C 77 47 58 6D 62 57 68 41 4D 6C  |VXJb0LwGXmbWhAMl|
```

```
0430  79 30 2F 4A 42 48 4C 4A 6E 59 77 44 78 73 4A 35  |y0/JBHLJnYwDxsJ5|
0440  47 72 6B 38 70 4F 69 54 4C 63 65 36 6C 52 6E 79  |Grk8pOiTLce6lRny|
0450  35 47 54 4E 78 50 6C 56 76 2F 4D 43 31 57 4E 6F  |5GTNxPlVv/MC1WNo|
0460  30 54 2F 54 34 71 7A 43 69 2B 41 4F 39 6C 37 74  |0T/T4qzCi+AO9l7t|
0470  57 67 51 43 36 78 72 62 36 36 49 54 34 4D 62 2B  |WgQC6xrb66IT4Mb+|
0480  46 58 45 37 6F 49 2F 34 37 72 44 75 69 32 4C 59  |FXE7oI/47rDui2LY|
0490  56 39 69 77 63 46 6F 57 35 76 46 6E 66 79 2B 48  |V9iwcFoW5vFnfy+H|
04A0  50 76 66 32 79 6E 7A 64 7A 2F 55 5A 6F 56 6F 69  |Pvf2ynzdz/UZoVoi|
04B0  2F 5A 57 5A 77 39 62 75 63 35 57 73 43 6E 6A 62  |/ZWZw9buc5WsCnjb|
04C0  6E 4B 52 59 70 33 6D 6E 36 68 59 4E 6E 59 5A 32  |nKRYp3mn6hYNnYZ2|
04D0  4E 35 50 75 66 43 47 43 46 47 49 57 6B 4B 4A 53  |N5PufCGCFGIWkKJS|
04E0  74 79 58 33 4C 55 64 54 4F 76 35 39 53 43 44 33  |tyX3LUdTOv59SCD3|
04F0  56 45 54 63 62 46 58 34 39 46 76 6B 30 61 65 37  |VETcbFX49Fvk0ae7|
0500  51 74 2F 38 42 76 42 4E 39 55 47 58 69 5A 71 6A  |Qt/8BvBN9UGXiZqj|
0510  71 50 49 4B 5A 6E 76 4E 69 59 36 68 6A 37 56 2F  |qPIKZnvNiY6hj7V/|
0520  69 4B 6D 6E 6B 68 30 2F 66 51 61 47 66 70 46 65  |iKmnkh0/fQaGfpFe|
0530  78 4C 50 61 6C 4B 77 6A 33 4F 39 4F 39 6E 43 2F  |xLPalKwj3O9O9nC/|
0540  52 4D 31 4C 73 37 6B 37 76 59 79 4F 43 61 2F 63  |RM1Ls7k7vYyOCa/c|
0550  6B 51 50 77 55 6E 72 31 59 6B 61 6A 57 30 4F 58  |kQPwUnr1YkajW0OX|
0560  61 55 46 52 33 43 46 4A 63 70 41 49 62 55 51 57  |aUFR3CFJcpAIbUQW|
0570  62 55 72 55 4F 59 62 46 32 77 66 6C 69 71 6E 72  |bUrUOYbF2wfliqnr|
0580  43 67 4A 6B 30 4D 64 31 62 38 39 62 42 52 71 32  |CgJk0Md1b89bBRq2|
0590  36 64 69 73 2B 5A 79 6E 78 66 36 59 35 32 59 31  |6dis+Zynxf6Y52Y1|
05A0  63 76 39 79 75 56 57 6F 76 77 4C 49 33 56 4F 53  |cv9yuVWovwLI3VOS|
05B0  52 2B 58 76 78 65 68 6A 59 51 71 68 2F 6A 65 54  |R+XvxehjYQqh/jeT|
05C0  37 70 59 74 57 55 58 49 54 76 46 6E 46 45 74 54  |7pYtWUXITvFnFEtT|
05D0  77 52 48 38 4D 47 58 73 34 65 46 70 46 66 67 6F  |wRH8MGXs4eFpFfgo|
05E0  4F 66 64 52 49 42 73 53 36 46 76 67 52 74 36 4A  |OfdRIBsS6FvgRt6J|
05F0  51 4A 48 6B 65 31 30 4C 6E 51 35 4C 4A 31 4C 71  |QJHke10LnQ5LJ1Lq|
0600  36 64 55 38 4A 74 68 33 59 37 43 71 37 39 6E 4E  |6dU8Jth3Y7Cq79nN|
0610  2B 53 53 75 38 4E 78 68 51 63 71 79 65 76 71 50  |+SSu8NxhQcqyevqP|
0620  65 38 76 76 56 62 6F 4E 72 69 4E 43 41 6E 35 61  |e8vvVboNriNCAn5a|
0630  6B 73 71 79 68 70 62 57 64 47 59 2B 55 6D 51 75  |ksqyhpbWdGY+UmQu|
0640  6B 30 71 47 31 44 50 5A 4D 58 6F 4F 52 31 74 79  |k0qG1DPZMXoOR1ty|
0650  74 74 59 79 65 42 30 35 67 6A 58 30 42 49 77 6D  |ttYyeB05gjX0BIwm|
0660  70 4C 2F 33 4F 2F 5A 62 4E 72 71 54 32 76 6C 35  |pL/3O/ZbNrqT2vl5|
0670  58 4B 69 41 57 48 44 31 76 32 44 6A 2F 72 70 5A  |XKiAWHD1v2Dj/rpZ|
0680  72 73 73 5A 78 35 38 67 32 2B 7A 61 63 4B 41 3D  |rssZx58g2+zacKA=|
0690  3D 3C 2F 43 65 72 74 3E 3C 53 67 6E 72 3E 3C 53  |=</Cert><Sgnr><S|
06A0  67 6E 72 49 64 3E 3C 49 73 73 72 41 6E 64 53 72  |gnrId><IssrAndSr|
06B0  6C 4E 62 3E 3C 49 73 73 72 3E 3C 52 6C 74 76 44  |lNb><Issr><RltvD|
06C0  73 74 6E 67 73 68 64 4E 6D 3E 3C 41 74 74 72 54  |stngshdNm><AttrT|
06D0  70 3E 43 41 54 54 3C 2F 41 74 74 72 54 70 3E 3C  |p>CATT</AttrTp><|
06E0  41 74 74 72 56 61 6C 3E 42 45 3C 2F 41 74 74 72  |AttrVal>BE</Attr|
06F0  56 61 6C 3E 3C 2F 52 6C 74 76 44 73 74 6E 67 73  |Val></RltvDstngs|
0700  68 64 4E 6D 3E 3C 52 6C 74 76 44 73 74 6E 67 73  |hdNm><RltvDstngs|
0710  68 64 4E 6D 3E 3C 41 74 74 72 54 70 3E 4F 41 54  |hdNm><AttrTp>OAT|
0720  54 3C 2F 41 74 74 72 54 70 3E 3C 41 74 74 72 56  |T</AttrTp><AttrV|
0730  61 6C 3E 45 50 41 53 4F 72 67 3C 2F 41 74 74 72  |al>EPASOrg</Attr|
0740  56 61 6C 3E 3C 2F 52 6C 74 76 44 73 74 6E 67 73  |Val></RltvDstngs|
0750  68 64 4E 6D 3E 3C 52 6C 74 76 44 73 74 6E 67 73  |hdNm><RltvDstngs|
0760  68 64 4E 6D 3E 3C 41 74 74 72 54 70 3E 4F 55 41  |hdNm><AttrTp>OUA|
0770  54 3C 2F 41 74 74 72 54 70 3E 3C 41 74 74 72 56  |T</AttrTp><AttrV|
0780  61 6C 3E 54 65 63 68 6E 69 63 61 6C 20 43 65 6E  |al>Technical Cen|
0790  74 65 72 20 6F 66 20 45 78 70 65 72 74 69 73 65  |ter of Expertise|
07A0  3C 2F 41 74 74 72 56 61 6C 3E 3C 2F 52 6C 74 76  |</AttrVal></Rltv|
07B0  44 73 74 6E 67 73 68 64 4E 6D 3E 3C 52 6C 74 76  |DstngshdNm><Rltv|
07C0  44 73 74 6E 67 73 68 64 4E 6D 3E 3C 41 74 74 72  |DstngshdNm><Attr|
07D0  54 70 3E 43 4E 41 54 3C 2F 41 74 74 72 54 70 3E  |Tp>CNAT</AttrTp>|
07E0  3C 41 74 74 72 56 61 6C 3E 45 50 41 53 20 50 72  |<AttrVal>EPAS Pr|
07F0  6F 74 6F 63 6F 6C 73 20 54 65 73 74 20 43 41 3C  |otocols Test CA<|
0800  2F 41 74 74 72 56 61 6C 3E 3C 2F 52 6C 74 76 44  |/AttrVal></RltvD|
0810  73 74 6E 67 73 68 64 4E 6D 3E 3C 2F 49 73 73 72  |stngshdNm></Issr|
0820  3E 3C 53 72 6C 4E 62 3E 49 69 57 6F 2B 77 41 48  |><SrlNb>IiWo+wAH|
0830  45 70 50 55 5A 42 77 38 3C 2F 53 72 6C 4E 62 3E  |EpPUZBw8</SrlNb>|
0840  3C 2F 49 73 73 72 41 6E 64 53 72 6C 4E 62 3E 3C  |</IssrAndSrlNb><|
0850  2F 53 67 6E 72 49 64 3E 3C 44 67 73 74 41 6C 67  |/SgnrId><DgstAlg|
0860  6F 3E 3C 41 6C 67 6F 3E 48 53 32 35 3C 2F 41 6C  |o><Algo>HS25</Al|
0870  67 6F 3E 3C 2F 44 67 73 74 41 6C 67 6F 3E 3C 53  |go></DgstAlgo><S|
```

```
0880  67 6E 74 72 41 6C 67 6F 3E 3C 41 6C 67 6F 3E 45  |gntrAlgo><Algo>E|
0890  52 53 32 3C 2F 41 6C 67 6F 3E 3C 2F 53 67 6E 74  |RS2</Algo></Sgnt|
08A0  72 41 6C 67 6F 3E 3C 53 67 6E 74 72 3E 62 67 35  |rAlgo><Sgntr>bg5|
08B0  58 42 39 2F 70 69 67 72 34 31 58 32 33 56 57 41  |XB9/pigr41X23VWA|
08C0  53 58 45 6C 36 6B 4A 68 50 35 30 34 47 6F 6C 51  |SXEl6kJhP504GolQ|
08D0  67 47 72 62 32 71 63 55 4E 42 4D 4B 64 36 2F 6F  |gGrb2qcUNBMKd6/o|
08E0  57 30 56 56 52 34 33 4D 62 63 42 33 44 79 6A 78  |W0VVR43MbcB3Dyjx|
08F0  39 79 6A 63 54 4C 38 57 77 73 33 31 4A 4D 72 34  |9yjcTL8Wws31JMr4|
0900  54 45 4D 35 35 7A 77 30 76 71 45 72 58 62 62 68  |TEM55zw0vqErXbbh|
0910  39 42 66 77 43 63 47 4F 79 54 66 36 68 69 4A 4B  |9BfwCcGOyTf6hiJK|
0920  6C 41 68 7A 6C 50 53 54 6D 68 74 68 57 52 62 64  |lAhzlPSTmhthWRbd|
0930  30 50 2B 53 6F 4C 52 58 4B 72 64 31 79 58 4B 30  |0P+SoLRXKrd1yXK0|
0940  34 48 73 65 68 72 65 65 6E 70 39 75 44 65 56 79  |4Hsehreenp9uDeVy|
0950  39 39 45 45 39 77 36 32 6B 31 6D 58 49 6D 36 32  |99EE9w62k1mXIm62|
0960  61 32 65 35 6F 6F 51 67 41 4A 31 2B 66 30 45 35  |a2e5ooQgAJ1+f0E5|
0970  4E 77 66 41 62 73 56 7A 75 41 71 42 2F 38 46 72  |NwfAbsVzuAqB/8Fr|
0980  2B 6A 6A 35 78 38 2B 63 77 51 41 70 57 51 64 46  |+jj5x8+cwQApWQdF|
0990  79 6C 53 32 67 63 6F 37 57 63 39 52 52 70 67 32  |ylS2gco7Wc9RRpg2|
09A0  58 2F 2F 32 76 6F 46 49 59 58 6F 52 44 6A 53 54  |X//2voFIYXoRDjST|
09B0  2B 30 79 6B 39 72 32 51 6C 51 2B 44 6D 50 43 33  |+0yk9r2QlQ+DmPC3|
09C0  65 30 4E 70 71 45 47 57 67 30 36 4B 4B 2B 51 52  |e0NpqEGWg06KK+QR|
09D0  49 61 70 43 2F 51 39 4B 71 49 31 67 4E 30 76 6F  |IapC/Q9KqI1gN0vo|
09E0  35 46 73 74 5A 4F 55 70 41 35 46 57 61 32 66 37  |5FstZOUpA5FWa2f7|
09F0  75 43 45 55 41 30 4D 62 67 51 64 2B 36 4A 50 49  |uCEUA0MbgQd+6JPI|
0A00  48 47 51 3D 3D 3C 2F 53 67 6E 74 72 3E 3C 2F 53  |HGQ==</Sgntr></S|
0A10  67 6E 72 3E 3C 2F 53 67 6E 64 44 61 74 61 3E 3C  |gnr></SgndData><|
0A20  2F 53 63 74 79 54 72 6C 72 3E                    |/SctyTrlr>      |
```

1.4.4 Management Plan with Key Download Action

In response to the *StatusReport* message containing no keys, the TM Host send a *ManagementPlanReplacement* message containing one immediate action to download the DUKPT initial key.

The header and the body of the *ManagementPlanReplacement* message is presented in the table below:

Message Item	*Value*
Header	
DownloadTransfer	True
FormatVersion	6.0
ExchangeIdentification	001
CreationDateTime	2013-12-06:13:53:52.00+02:00
InitiatingParty	
Identification	66000001
Type	OriginationgPOI
Issuer	MasterTerminalManager
RecipientParty	
Identification	epas-keyDownload-TM1
Type	MasterTerminalManager
ManagementPlan	
POIIdentification	
Identification	66000001
Type	OriginationgPOI
Issuer	MasterTerminalManager
TerminalManagerdentification	
Identification	epas-keyDownload-TM1
Type	MasterTerminalManager
DataSet	
Identification	
Type	ManagementPlan
CreationDateTime	2013-12-06:13:53:52.00+02:00
Content	
Action	
Type	Download
DataSetIdentification	
Name	epas-acquirer-TM1-TIK
Type	SecurityParameters
Version	20131206135352
Trigger	DateTime
AdditionalProcess	Restart
Retry	
Delay	10
MaximumNumber	2
TimeCondition	
StartTime	2013-12-06:13:53:49
TMChallenge	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
KeyEnciphrementCertificate	30820501308202E9A003020102020C7895CA35014C3D2F1E11B10D300D06092A864886F70D01010B05003068310B300906035504060C0242453110300E060355040A0C07455041534F7267312630240603550 40B0C1D546563686E6963616C2043656E746572206F662045787065 7274697365311F301D06035504030C16455041532050726F746F636 F6C732054657374204341302A181332303133303431383130313832

	332B303130301813323031383130303131383230303052B303130303 078310B300906035504060C0246523110300E060355040A0C074550 41534F726731263024060355040B0C1D546563686E6963616C20436 56E746572206F662045787065727469736531 2F302D06035504030C 2645504153205072 6F746F636F6C205465737420486F7374204B657 920456E6372797074696F6E308201A2300D06092A864886F70D0101 0105000382018F003082018A0282018100D72CCF63FB2F866A18F21 9DC919316495FF66C906F904D7B266525C37FABE7D4ED99EA042433 6D99B0B7979DE1764E7CD16B64B9BA954610BCACBB6CFDA4CB906AA 75BED58B9A0037152541EB1DC3DD0B6214EB31BE97A4F91073412DE 042216FA8F826D24C7F2D305D4BF63465BF899DC6F073FF6AA338EA 44DB6BE51A6358CAA3CCB8528E58B55540ED22325233333D3D6D2B8 2ED7A58D499F445FF835C3EBD5B515379A7C2B5B41D35F3DFD5A1A2 D61491038FDD19E18EF678FD794872ACC8B8129AFA0D02FCD6E4ADE 9184D5FEC2386441293B16BB76B8E2E4F8E80276366855A880E0EFA C449E76124C4BF7FF2BA15E674B62A5637D26600AA3A013E1530E11 F4BF984E533F520A2E74BD826DD507C283D2F563C22848E05D84D2B 7D2221F4B63B56797E6AFB425D567E5F916E3AB4E2C486EC8148946 9C17DA2DFAF7AB496EE7C24E43951FFE28006BFF96E2D15838AC725 2F3D45E8FEBEF0F7EEF974FFE0A38C38926CFA0683198CA8FD08C8B 2427B91A0B16F79A7186DE7DAB9DFF3D0203010001A30F300D300B0 603551D0F040403020520300D06092A864886F70D01010B05000382 02010026ED5F4E115A9E2D10F07B35D10F35D8BD3BB40D481E5F0D2 E08C80241D70002BA5C7307491CE28953CB70D49D85D20D0BBAFDBD C404EFB7AEDD2B5E9292EA7684783E02DC98955CFB1D941719E1E48 FF83F1174102435B35259E7509F8FB67C30DDBEE7B5F540AD890035 D604B98D2F0814E78F8F9DE9D4B77AF726DB667CCAF70A175AF87F7 16979CA8783A8247E3CF36BD8DC316FE1D631A24896253D1242AE65 9E3EA15A82E73C4B296457AF5F088B00F6EF51730EE5E4FA9BAF6ED 8E4CC34F0FB90FF4442D455F3619A5059CA82DD15CB401302E70F12 4BDE6D514156FB42DDE6ADA620EF2D27B7F2189B4FCAB9F4487DA26 ED4418F00EA4C7A89308EAC88E5865943F95F087A6FB7749BDB783E 2AE28FF7C410ADC935F41658F36CD90F2CC895A27DB5AD1EF147AA6 0634A6591C343AC7FF95C6D7D7CB88EBB361691FDA586551D6F0CAD 7FE5F037460350E5D0A650D627EB0C1B5315B0492414684230BBA23 9D5CAB98942079DAB4F0CBBCEB2D881D0FFE8B2E19DB8F94AE9D99B AC6BE2C48E5FE45DEEC2FFE8FAF52B43256BC50E17F0CEF1AB8B869 4FC3493627CF2852283B25176DDAFEE8FBA49F434D2B7F1BCAF79CC B3EAD15F3A6D11939EDC406352DF6A68F1201831CED0FE205E1F381 5F46E01E6E5F5798DE2EFB7CF6EFE578BA33AEDBB3ED9C4EF39EA5E 9A6899CE00DB6C8922450AA18227549DB43F1643

As for the previous message, the POI has no symmetric key shared usable by the key injection, so the TM authentication RSA key is used to provide a digital signature of the message body.

Once unnecessary spaces and carriage returns are removed, the XML encoded *ManagementPlanReplacement* message body is:

```
0000  3C 4D 67 6D 74 50 6C 61 6E 3E 3C 50 4F 49 49 64  |<MgmtPlan><POIId|
0010  3E 3C 49 64 3E 36 36 30 30 30 30 30 31 3C 2F 49  |><Id>66000001</I|
0020  64 3E 3C 54 70 3E 4F 50 4F 49 3C 2F 54 70 3E 3C  |d><Tp>OPOI</Tp><|
0030  49 73 73 72 3E 4D 54 4D 47 3C 2F 49 73 73 72 3E  |Issr>MTMG</Issr>|
0040  3C 2F 50 4F 49 49 64 3E 3C 54 65 72 6D 6E 6C 4D  |</POIId><TermnlM|
0050  67 72 49 64 3E 3C 49 64 3E 65 70 61 73 2D 6B 65  |grId><Id>epas-ke|
0060  79 44 6F 77 6E 6C 6F 61 64 2D 54 4D 31 3C 2F 49  |yDownload-TM1</I|
0070  64 3E 3C 54 70 3E 4D 54 4D 47 3C 2F 54 70 3E 3C  |d><Tp>MTMG</Tp><|
0080  2F 54 65 72 6D 6E 6C 4D 67 72 49 64 3E 3C 44 61  |/TermnlMgrId><Da|
0090  74 61 53 65 74 3E 3C 49 64 3E 3C 54 70 3E 4D 47  |taSet><Id><Tp>MG|
00A0  54 50 3C 2F 54 70 3E 3C 43 72 65 44 74 54 6D 3E  |TP</Tp><CreDtTm>|
00B0  32 30 31 33 2D 31 32 2D 30 36 54 31 33 3A 35 33  |2013-12-06T13:53|
00C0  3A 35 32 2E 30 30 2B 30 32 3A 30 30 3C 2F 43 72  |:52.00+02:00</Cr|
00D0  65 44 74 54 6D 3E 3C 2F 49 64 3E 3C 43 6E 74 74  |eDtTm></Id><Cntt|
00E0  3E 3C 41 63 74 6E 3E 3C 54 70 3E 44 57 4E 4C 3C  |><Actn><Tp>DWNL<|
00F0  2F 54 70 3E 3C 44 61 74 61 53 65 74 49 64 3E 3C  |/Tp><DataSetId><|
0100  4E 6D 3E 65 70 61 73 2D 61 63 71 75 69 72 65 72  |Nm>epas-acquirer|
0110  2D 54 4D 31 2D 54 49 4B 3C 2F 4E 6D 3E 3C 54 70  |-TM1-TIK</Nm><Tp|
0120  3E 53 43 50 52 3C 2F 54 70 3E 3C 56 72 73 6E 3E  |>SCPR</Tp><Vrsn>|
0130  32 30 31 33 31 32 30 36 31 33 35 33 35 32 3C 2F  |20131206135352</|
0140  56 72 73 6E 3E 3C 2F 44 61 74 61 53 65 74 49 64  |Vrsn></DataSetId|
0150  3E 3C 54 72 67 67 72 3E 44 41 54 45 3C 2F 54 72  |><Trggr>DATE</Tr|
0160  67 67 72 3E 3C 41 64 64 74 6C 50 72 63 3E 52 53  |ggr><AddtlPrc>RS|
0170  52 54 3C 2F 41 64 64 74 6C 50 72 63 3E 3C 52 65  |RT</AddtlPrc><Re|
0180  54 72 79 3E 3C 44 65 6C 79 3E 31 30 3C 2F 44 65  |Try><Dely>10</De|
0190  6C 79 3E 3C 4D 61 78 4E 62 3E 32 3C 2F 4D 61 78  |ly><MaxNb>2</Max|
01A0  4E 62 3E 3C 2F 52 65 54 72 79 3E 3C 54 6D 43 6F  |Nb></ReTry><TmCo|
01B0  6E 64 3E 3C 53 74 61 72 74 54 6D 3E 32 30 31 33  |nd><StartTm>2013|
01C0  2D 31 32 2D 30 36 54 31 33 3A 35 33 3A 34 39 3C  |-12-06T13:53:49<|
01D0  2F 53 74 61 72 74 54 6D 3E 3C 2F 54 6D 43 6F 6E  |/StartTm></TmCon|
01E0  64 3E 3C 54 4D 43 68 6C 6C 6E 67 3E 34 37 44 45  |d><TMChllng>47DE|
01F0  51 70 6A 38 48 42 53 61 2B 2F 54 49 6D 57 2B 35  |Qpj8HBSa+/TImW+5|
0200  4A 43 65 75 51 65 52 6B 6D 35 4E 4D 70 4A 57 5A  |JCeuQeRkm5NMpJWZ|
0210  47 33 68 53 75 46 55 3D 3C 2F 54 4D 43 68 6C 6C  |G3hSuFU=</TMChll|
0220  6E 67 3E 3C 4B 65 79 4E 63 70 68 72 6D 6E 74 43  |ng><KeyNcphrmntC|
0230  65 72 74 3E 4D 49 49 46 41 54 43 43 41 75 6D 67  |ert>MIIFATCCAumg|
0240  41 77 49 42 41 67 49 4D 65 4A 58 4B 4E 51 46 4D  |AwIBAgIMeJXKNQFM|
0250  50 53 38 65 45 62 45 4E 4D 41 30 47 43 53 71 47  |PS8eEbENMA0GCSqG|
0260  53 49 62 33 44 51 45 42 43 77 55 41 4D 47 67 78  |SIb3DQEBCwUAMGgx|
0270  43 7A 41 4A 42 67 4E 56 42 41 59 4D 41 6B 4A 46  |CzAJBgNVBAYMAkJF|
0280  4D 52 41 77 44 67 59 44 56 51 51 4B 44 41 64 46  |MRAwDgYDVQQKDAdF|
0290  55 45 46 54 54 33 4A 6E 4D 53 59 77 4A 41 59 44  |UEFTT3JnMSYwJAYD|
02A0  56 51 51 4C 44 42 31 55 5A 57 4E 6F 62 6D 6C 6A  |VQQLDB1UZWNobmlj|
02B0  59 57 77 67 51 32 56 75 64 47 56 79 49 47 39 6D  |YWwgQ2VudGVyIG9m|
02C0  49 45 56 34 63 47 56 79 64 47 6C 7A 5A 54 45 66  |IEV4cGVydGlzZTEf|
02D0  4D 42 30 47 41 31 55 45 41 77 77 57 52 56 42 42  |MB0GA1UEAwwWRVBB|
02E0  55 79 42 51 63 6D 39 30 62 32 4E 76 62 48 4D 67  |UyBQcm90b2NvbHMg|
02F0  56 47 56 7A 64 43 42 44 51 54 41 71 47 42 4D 79  |VGVzdCBDQTAqGBMy|
```

```
0300  4D 44 45 7A 4D 44 51 78 4F 44 45 77 4D 54 67 79  |MDEzMDQxODEwMTgy|
0310  4D 79 73 77 4D 54 41 77 47 42 4D 79 4D 44 45 34  |MyswMTAwGBMyMDE4|
0320  4D 54 41 77 4D 54 45 34 4D 6A 41 77 4E 53 73 77  |MTAwMTE4MjAwNSsw|
0330  4D 54 41 77 4D 48 67 78 43 7A 41 4A 42 67 4E 56  |MTAwMHgxCzAJBgNV|
0340  42 41 59 4D 41 6B 5A 53 4D 52 41 77 44 67 59 44  |BAYMAkZSMRAwDgYD|
0350  56 51 51 4B 44 41 64 46 55 45 46 54 54 33 4A 6E  |VQQKDAdFUEFTT3Jn|
0360  4D 53 59 77 4A 41 59 44 56 51 51 4C 44 42 31 55  |MSYwJAYDVQQLDB1U|
0370  5A 57 4E 6F 62 6D 6C 6A 59 57 77 67 51 32 56 75  |ZWNobmljYWwgQ2Vu|
0380  64 47 56 79 49 47 39 6D 49 45 56 34 63 47 56 79  |dGVyIG9mIEV4cGVy|
0390  64 47 6C 7A 5A 54 45 76 4D 43 30 47 41 31 55 45  |dGlzZTEvMC0GA1UE|
03A0  41 77 77 6D 52 56 42 42 55 79 42 51 63 6D 39 30  |AwwmRVBBUyBQcm90|
03B0  62 32 4E 76 62 43 42 55 5A 58 4E 30 49 45 68 76  |b2NvbCBUZXN0IEhv|
03C0  63 33 51 67 53 32 56 35 49 45 56 75 59 33 4A 35  |c3QgS2V5IEVuY3J5|
03D0  63 48 52 70 62 32 34 77 67 67 47 69 4D 41 30 47  |cHRpb24wggGiMA0G|
03E0  43 53 71 47 53 49 62 33 44 51 45 42 41 51 55 41  |CSqGSIb3DQEBAQUA|
03F0  41 34 49 42 6A 77 41 77 67 67 47 4B 41 6F 49 42  |A4IBjwAwggGKAoIB|
0400  67 51 44 58 4C 4D 39 6A 2B 79 2B 47 61 68 6A 79  |gQDXLM9j+y+Gahjy|
0410  47 64 79 52 6B 78 5A 4A 58 2F 5A 73 6B 47 2B 51  |GdyRkxZJX/ZskG+Q|
0420  54 58 73 6D 5A 53 58 44 66 36 76 6E 31 4F 32 5A  |TXsmZSXDf6vn1O2Z|
0430  36 67 51 6B 4D 32 32 5A 73 4C 65 58 6E 65 46 32  |6gQkM22ZsLeXneF2|
0440  54 6E 7A 52 61 32 53 35 75 70 56 47 45 4C 79 73  |TnzRa2S5upVGELys|
0450  75 32 7A 39 70 4D 75 51 61 71 64 62 37 56 69 35  |u2z9pMuQaqdb7Vi5|
0460  6F 41 4E 78 55 6C 51 65 73 64 77 39 30 4C 59 68  |oANxUlQesdw90LYh|
0470  54 72 4D 62 36 58 70 50 6B 51 63 30 45 74 34 45  |TrMb6XpPkQc0Et4E|
0480  49 68 62 36 6A 34 4A 74 4A 4D 66 79 30 77 58 55  |Ihb6j4JtJMfy0wXU|
0490  76 32 4E 47 57 2F 69 5A 33 47 38 48 50 2F 61 71  |v2NGW/iZ3G8HP/aq|
04A0  4D 34 36 6B 54 62 61 2B 55 61 59 31 6A 4B 6F 38  |M46kTba+UaY1jKo8|
04B0  79 34 55 6F 35 59 74 56 56 41 37 53 49 79 55 6A  |y4Uo5YtVVA7SIyUj|
04C0  4D 7A 50 54 31 74 4B 34 4C 74 65 6C 6A 55 6D 66  |MzPT1tK4LteljUmf|
04D0  52 46 2F 34 4E 63 50 72 31 62 55 56 4E 35 70 38  |RF/4NcPr1bUVN5p8|
04E0  4B 31 74 42 30 31 38 39 2F 56 6F 61 4C 57 46 4A  |K1tB0189/VoaLWFJ|
04F0  45 44 6A 39 30 5A 34 59 37 32 65 50 31 35 53 48  |EDj90Z4Y72eP15SH|
0500  4B 73 79 4C 67 53 6D 76 6F 4E 41 76 7A 57 35 4B  |KsyLgSmvoNAvzW5K|
0510  33 70 47 45 31 66 37 43 4F 47 52 42 4B 54 73 57  |3pGE1f7COGRBKTsW|
0520  75 33 61 34 34 75 54 34 36 41 4A 32 4E 6D 68 56  |u3a44uT46AJ2NmhV|
0530  71 49 44 67 37 36 78 45 6E 6E 59 53 54 45 76 33  |qIDg76xEnnYSTEv3|
0540  2F 79 75 68 58 6D 64 4C 59 71 56 6A 66 53 5A 67  |/yuhXmdLYqVjfSZg|
0550  43 71 4F 67 45 2B 46 54 44 68 48 30 76 35 68 4F  |CqOgE+FTDhH0v5hO|
0560  55 7A 39 53 43 69 35 30 76 59 4A 74 31 51 66 43  |Uz9SCi50vYJt1QfC|
0570  67 39 4C 31 59 38 49 6F 53 4F 42 64 68 4E 4B 33  |g9L1Y8IoSOBdhNK3|
0580  30 69 49 66 53 32 4F 31 5A 35 66 6D 72 37 51 6C  |0iIfS2O1Z5fmr7Ql|
0590  31 57 66 6C 2B 52 62 6A 71 30 34 73 53 47 37 49  |1Wfl+Rbjq04sSG7I|
05A0  46 49 6C 47 6E 42 66 61 4C 66 72 33 71 30 6C 75  |FIlGnBfaLfr3q0lu|
05B0  35 38 4A 4F 51 35 55 66 2F 69 67 41 61 2F 2B 57  |58JOQ5Uf/igAa/+W|
05C0  34 74 46 59 4F 4B 78 79 55 76 50 55 58 6F 2F 72  |4tFYOKxyUvPUXo/r|
05D0  37 77 39 2B 37 35 64 50 2F 67 6F 34 77 34 6B 6D  |7w9+75dP/go4w4km|
05E0  7A 36 42 6F 4D 5A 6A 4B 6A 39 43 4D 69 79 51 6E  |z6BoMZjKj9CMiyQn|
05F0  75 52 6F 4C 46 76 65 61 63 59 62 65 66 61 75 64  |uRoLFveacYbefaud|
0600  2F 7A 30 43 41 77 45 41 41 61 4D 50 4D 41 30 77  |/z0CAwEAAaMPMA0w|
0610  43 77 59 44 56 52 30 50 42 41 51 44 41 67 55 67  |CwYDVR0PBAQDAgUg|
0620  4D 41 30 47 43 53 71 47 53 49 62 33 44 51 45 42  |MA0GCSqGSIb3DQEB|
0630  43 77 55 41 41 34 49 43 41 51 41 6D 37 56 39 4F  |CwUAA4ICAQAm7V9O|
0640  45 56 71 65 4C 52 44 77 65 7A 58 52 44 7A 58 59  |EVqeLRDwezXRDzXY|
0650  76 54 75 30 44 55 67 65 58 77 30 75 43 4D 67 43  |vTu0DUgeXw0uCMgC|
```

```
0660  51 64 63 41 41 72 70 63 63 77 64 4A 48 4F 4B 4A  |QdcAArpccwdJHOKJ|
0670  55 38 74 77 31 4A 32 46 30 67 30 4C 75 76 32 39  |U8tw1J2F0g0Luv29|
0680  78 41 54 76 74 36 37 64 4B 31 36 53 6B 75 70 32  |xATvt67dK16Skup2|
0690  68 48 67 2B 41 74 79 59 6C 56 7A 37 48 5A 51 58  |hHg+AtyYlVz7HZQX|
06A0  47 65 48 6B 6A 2F 67 2F 45 58 51 51 4A 44 57 7A  |GeHkj/g/EXQQJDWz|
06B0  55 6C 6E 6E 55 4A 2B 50 74 6E 77 77 33 62 37 6E  |UlnnUJ+Ptnww3b7n|
06C0  74 66 56 41 72 59 6B 41 4E 64 59 45 75 59 30 76  |tfVArYkANdYEuY0v|
06D0  43 42 54 6E 6A 34 2B 64 36 64 53 33 65 76 63 6D  |CBTnj4+d6dS3evcm|
06E0  32 32 5A 38 79 76 63 4B 46 31 72 34 66 33 46 70  |22Z8yvcKF1r4f3Fp|
06F0  65 63 71 48 67 36 67 6B 66 6A 7A 7A 61 39 6A 63  |ecqHg6gkfjzza9jc|
0700  4D 57 2F 68 31 6A 47 69 53 4A 59 6C 50 52 4A 43  |MW/h1jGiSJYlPRJC|
0710  72 6D 57 65 50 71 46 61 67 75 63 38 53 79 6C 6B  |rmWePqFaguc8Sylk|
0720  56 36 39 66 43 49 73 41 39 75 39 52 63 77 37 6C  |V69fCIsA9u9Rcw7l|
0730  35 50 71 62 72 32 37 59 35 4D 77 30 38 50 75 51  |5Pqbr27Y5Mw08PuQ|
0740  2F 30 52 43 31 46 58 7A 59 5A 70 51 57 63 71 43  |/0RC1FXzYZpQWcqC|
0750  33 52 58 4C 51 42 4D 43 35 77 38 53 53 39 35 74  |3RXLQBMC5w8SS95t|
0760  55 55 46 57 2B 30 4C 64 35 71 32 6D 49 4F 38 74  |UUFW+0Ld5q2mIO8t|
0770  4A 37 66 79 47 4A 74 50 79 72 6E 30 53 48 32 69  |J7fyGJtPyrn0SH2i|
0780  62 74 52 42 6A 77 44 71 54 48 71 4A 4D 49 36 73  |btRBjwDqTHqJMI6s|
0790  69 4F 57 47 57 55 50 35 58 77 68 36 62 37 64 30  |iOWGWUP5Xwh6b7d0|
07A0  6D 39 74 34 50 69 72 69 6A 2F 66 45 45 4B 33 4A  |m9t4Pirij/fEEK3J|
07B0  4E 66 51 57 57 50 4E 73 32 51 38 73 79 4A 57 69  |NfQWWPNs2Q8syJWi|
07C0  66 62 57 74 48 76 46 48 71 6D 42 6A 53 6D 57 52  |fbWtHvFHqmBjSmWR|
07D0  77 30 4F 73 66 2F 6C 63 62 58 31 38 75 49 36 37  |w0Osf/lcbX18uI67|
07E0  4E 68 61 52 2F 61 57 47 56 52 31 76 44 4B 31 2F  |NhaR/aWGVR1vDK1/|
07F0  35 66 41 33 52 67 4E 51 35 64 43 6D 55 4E 59 6E  |5fA3RgNQ5dCmUNYn|
0800  36 77 77 62 55 78 57 77 53 53 51 55 61 45 49 77  |6wwbUxWwSSQUaEIw|
0810  75 36 49 35 31 63 71 35 69 55 49 48 6E 61 74 50  |u6I51cq5iUIHnatP|
0820  44 4C 76 4F 73 74 69 42 30 50 2F 6F 73 75 47 64  |DLvOstiB0P/osuGd|
0830  75 50 6C 4B 36 64 6D 62 72 47 76 69 78 49 35 66  |uPlK6dmbrGvixI5f|
0840  35 46 33 75 77 76 2F 6F 2B 76 55 72 51 79 56 72  |5F3uwv/o+vUrQyVr|
0850  78 51 34 58 38 4D 37 78 71 34 75 47 6C 50 77 30  |xQ4X8M7xq4uGlPw0|
0860  6B 32 4A 38 38 6F 55 69 67 37 4A 52 64 74 32 76  |k2J88oUig7JRdt2v|
0870  37 6F 2B 36 53 66 51 30 30 72 66 78 76 4B 39 35  |7o+6SfQ00rfxvK95|
0880  7A 4C 50 71 30 56 38 36 62 52 47 54 6E 74 78 41  |zLPq0V86bRGTntxA|
0890  59 31 4C 66 61 6D 6A 78 49 42 67 78 7A 74 44 2B  |Y1LfamjxIBgxztD+|
08A0  49 46 34 66 4F 42 58 30 62 67 48 6D 35 66 56 35  |IF4fOBX0bgHm5fV5|
08B0  6A 65 4C 76 74 38 39 75 2F 6C 65 4C 6F 7A 72 74  |jeLvt89u/leLozrt|
08C0  75 7A 37 5A 78 4F 38 35 36 6C 36 61 61 4A 6E 4F  |uz7ZxO856l6aaJnO|
08D0  41 4E 74 73 69 53 4A 46 43 71 47 43 4A 31 53 64  |ANtsiSJFCqGCJ1Sd|
08E0  74 44 38 57 51 77 3D 3D 3C 2F 4B 65 79 4E 63 70  |tD8WQw==</KeyNcp|
08F0  68 72 6D 6E 74 43 65 72 74 3E 3C 2F 41 63 74 6E  |hrmntCert></Actn|
0900  3E 3C 2F 43 6E 74 74 3E 3C 2F 44 61 74 61 53 65  |></Cntt></DataSe|
0910  74 3E 3C 2F 4D 67 6D 74 50 6C 61 6E 3E           |t></MgmtPlan>   |
```

The SHA256 digest of the *ManagementPlanReplacement* message body is:

```
0000  CF 04 10 CC DF F0 0E C7 FA A4 C9 2F 2B 5F E9 93  |............./+_..|
0010  5C 85 A0 E0 27 49 D2 93 94 76 58 96 5A 28 AF 4E  |\...'I...vX.Z(.N|
```

Applying the padding process for the digital signature, the block result is dumped below:

```
0000  00 01 FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0010  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0020  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0030  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0040  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0050  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0060  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0070  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0080  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0090  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
00A0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
00B0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
00C0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
00D0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
00E0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
00F0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0100  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0110  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0120  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0130  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0140  FF FF FF FF FF FF FF FF FF FF FF FF FF 00 30 31 30  |.............010|
0150  0D 06 09 60 86 48 01 65 03 04 02 01 05 00 04 20  |...`.H.e....... |
0160  CF 04 10 CC DF F0 0E C7 FA A4 C9 2F 2B 5F E9 93  |.........../+_..|
0170  5C 85 A0 E0 27 49 D2 93 94 76 58 96 5A 28 AF 4E  |\...'I...vX.Z(.N|
```

After encryption by the private key of $K_{TM\text{-}Sign}$, we have the digital signature of the *ManagementPlanReplacement* message body:

```
0000  81 1E 2B 38 75 85 ED D4 91 C8 1B 79 CE FF F1 92  |..+8u......y....|
0010  7A 95 73 A6 99 4D 19 C8 EF 88 12 BE E7 B9 79 E8  |z.s..M........y.|
0020  83 8B DA CA 94 5B 5B 9F 46 A0 1A 33 58 2B 63 E5  |.....[[.F..3X+c.|
0030  6A 16 46 1F 1A 30 4F E6 4C 2B 47 72 AF C7 5E 08  |j.F..0O.L+Gr..^.|
0040  34 C4 5F 76 DF 33 82 83 8E 4E E1 FA 91 ED 95 3C  |4._v.3...N.....<|
0050  2E F3 E7 29 7B B1 41 AF BC 46 14 9D D8 5A 4A 2A  |...){.A..F...ZJ*|
0060  B8 CF B3 35 78 3F 80 1B 86 93 0A C5 CD AE C1 1B  |...5x?..........|
0070  3F 31 5F BE 7F E9 E3 6F 2B 4A 2F BE 82 61 BB 98  |?1_....o+J/..a..|
0080  16 76 28 A2 75 E7 43 DB C6 87 50 ED 7C 34 4A 3B  |.v(.u.C...P.|4J;|
0090  01 F0 E1 57 1F 91 56 4E 35 24 10 43 9F A9 54 B2  |...W..VN5$.C..T.|
00A0  58 7C 22 16 37 28 CB D3 BB DD D1 20 2A 83 1B F2  |X|".7(..... *...|
00B0  C8 12 CB E8 50 60 E5 AA 60 05 DE 60 31 8D 70 B1  |....P`..`..`1.p.|
00C0  AA A5 24 03 25 03 48 9F 92 68 DA CE C4 C6 C1 A8  |..$.%.H..h......|
00D0  FA 50 54 33 18 0E 07 76 17 CF 79 98 51 E6 2A A2  |.PT3...v..y.Q.*.|
00E0  2D 0B 64 7C AD 67 8A 6B 10 AD 01 BD F7 16 78 20  |-.d|.g.k......x |
00F0  81 FA 99 C1 3D AF F6 06 46 ED AC 7A 8D 94 29 0F  |....=...F..z..).|
0100  7B 2F F9 E3 9C B2 6B 7F EA D6 D2 E9 66 30 DE 14  |{/....k.....f0..|
0110  E6 20 A7 B9 B5 F5 CB B9 01 AD 81 17 31 E3 4F 25  |. ..........1.O%|
0120  C7 73 70 1D C2 C5 37 F8 74 79 64 F7 F0 59 2A 99  |.sp...7.tyd..Y*.|
0130  AC 6E AD 2E 39 08 41 CE 4C E0 21 1A 47 66 A1 62  |.n..9.A.L.!.Gf.b|
0140  D2 B0 14 B4 6A 1E 1C 5A BC 41 36 01 A7 07 97 A1  |....j..Z.A6.....|
0150  78 C5 B0 40 AD 74 B4 B3 1D 4C DE D1 B7 96 AC E7  |x..@.t...L......|
0160  34 BF FE 3C 33 B0 A2 79 09 71 F8 24 FF C0 9F AD  |4..<3..y.q.$....|
0170  28 60 28 B1 46 53 5D 5F CD 48 60 E7 7F 9F 01 DC  |(`(.FS]_.H`.....|
```

Inside the *SecurityTrailer*, the *SignedData* CMS data structure is presented in the table below:

Message Item	*Value*
SecurityTrailer	
SignedData	
ContentType	SignedData
DigestAlgorithm	
Algorithm	SHA256
EncapsulatedContent	
ContentType	PlainData
Certificate	308204FF308202E7A003020102020A2ABC40F4D482F5EBC975300D06092A8648 86F70D01010B05003068310B300906035504060C0242453110300E060355040A 0C07455041534F726731263024060355040B0C1D546563686E6963616C204365 6E746572206F66204578706572746973653 11F301D06035504030C1645504153 2050726F746F636F6C732054657374204341302A181332303133303431383130 303634362B303130301813323031383130303131383230303052B303130303078 310B300906035504060C0246523110300E060355040A0C07455041534F726731 263024060355040B0C1D546563686E6963616C2043656E746572206F66204578 706572746973653 12F302D06035504030C2645504153205072 6F746F636F6C20 5465737420486F737420417574686E7469636174696F6E308201A2300D0609 2A864886F70D01010105000382018F003082018A0282018100BD095898F981BA F42BE20E19339B396C59626690BDF396D20C503CA57C688AF41E50552CF1B9DD C4116209DD00C26B673F7EDEE7D0CA6DC2DAA9FF2F8C3A860B8F835AE60D9E05 7EDDF1625FAC55A102837FC1C7EF8C0A6C137C5973972ABC40F4D482F5EBC975 4F964B6EECEDBE66DB62AD0DA7B38E05917562E899DF717D27457693B41E7BF2 CBA98855AE2C97DE4B48FD812A520D6D356010F6E8355EC98DBA3047F2C0CDCD 9BE655277F3ED69A788DD80A6A12BCA3D4C7F08662B99D3F70A9548D7804B5E4 A2913A3EC02525BE639ED7D9B986556C5932675642FCC4E659D828A94C5544AE BBC5446EE6B96A04A0185470296DFC2FFBA73D4074930968DD810E43D574DD7B E664899DA6E48EB4B3B590E2CAA97C75015C735093AD62E3FD791AB5718F1FA1
Signer	
SignerIdentification	
IssuerAnd-SerialNumber	
Issuer	
RelativeDistin-guishedName	
AttributeType	CountryName
AttributeValue	BE
RelativeDistin-guishedName	
AttributeType	OrganisationName
AttributeValue	EPASOrg
RelativeDistin-guishedName	
AttributeType	OrganisationUnitName
AttributeValue	Technical Center of Expertise
RelativeDistin-guishedName	
AttributeType	CommonName
AttributeValue	EPAS Protocols Test CA
SerialNumber	2ABC40F4D482F5EBC975
DigestAlgorithm	
Algorithm	SHA256
SignatureAlgorithm	
Algorithm	SHA256WithRSA

Signature	811E2B387585EDD491C81B79CEFFF1927A9573A6994D19C8EF8812BEE7B979E8 838BDACA945B5B9F46A01A33582B63E56A16461F1A304FE64C2B4772AFC75E08 34C45F76DF3382838E4EE1FA91ED953C2EF3E7297BB141AFBC46149DD85A4A2A B8CFB335783F801B86930AC5CDAEC11B3F315FBE7FE9E36F2B4A2FBE8261BB98 167628A275E743DBC68750ED7C344A3B01F0E1571F91564E352410439FA954B2 587C22163728CBD3BBDDD1202A831BF2C812CBE85060E5AA6005DE60318D70B1 AAA524032503489F9268DACEC4C6C1A8FA505433180E077617CF799851E62AA2 2D0B647CAD678A6B10AD01BDF716782081FA99C13DAFF60646EDAC7A8D94290F 7B2FF9E39CB26B7FEAD6D2E96630DE14E620A7B9B5F5CBB901AD811731E34F25 C773701DC2C537F8747964F7F0592A99AC6EAD2E390841CE4CE0211A4766A162 D2B014B46A1E1C5ABC413601A70797A178C5B040AD74B4B31D4CDED1B796ACE7 34BFFE3C33B0A2790971F824FFC09FAD286028B146535D5FCD4860E77F9F01DC

The XML encoded structure of the *ManagementPlanReplacement* message is:

```
<?xml version="1.0" encoding="UTF-8"?>
<Document xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="urn:iso:std:iso:20022:tech:xsd:catm.002.001.06">
 <MgmtPlanRplcmnt>
   <Hdr>
     <DwnldTrf>true</DwnldTrf>
     <FrmtVrsn>6.0</FrmtVrsn>
     <XchgId>001</XchgId>
     <CreDtTm>2013-12-06T13:53:52.00+02:00</CreDtTm>
     <InitgPty>
       <Id>66000001</Id>
       <Tp>OPOI</Tp>
       <Issr>MTMG</Issr>
     </InitgPty>
     <RcptPty>
       <Id>epas-keyDownload-TM1</Id>
       <Tp>MTMG</Tp>
     </RcptPty>
   </Hdr>
   <MgmtPlan>
     <POIId>
       <Id>66000001</Id>
       <Tp>OPOI</Tp>
       <Issr>MTMG</Issr>
     </POIId>
     <TermnlMgrId>
       <Id>epas-keyDownload-TM1</Id>
       <Tp>MTMG</Tp>
     </TermnlMgrId>
     <DataSet>
       <Id>
         <Tp>MGTP</Tp>
         <CreDtTm>2013-12-06T13:53:52.00+02:00</CreDtTm>
       </Id>
       <Cntt>
         <Actn>
           <Tp>DWNL</Tp>
           <DataSetId>
             <Nm>epas-acquirer-TM1-TIK</Nm>
             <Tp>SCPR</Tp>
             <Vrsn>20131206135352</Vrsn>
           </DataSetId>
           <Trggr>DATE</Trggr>
           <AddtlPrc>RSRT</AddtlPrc>
           <ReTry>
             <Dely>10</Dely>
             <MaxNb>2</MaxNb>
           </ReTry>
           <TmCond>
             <StartTm>2013-12-06T13:53:49</StartTm>
           </TmCond>
           <TMChllng>
```

```
                47DEQpj8HBSa+/TImW+5JCeuQeRkm5NMpJWZG3hSuFU=
            </TMChllng>
            <KeyNcphrmntCert>
              MIIFATCCAumgAwIBAgIMeJXKNQFMPS8eEbENMA0GCSqGSIb3DQEBCwUAMGgxCzAJBgNVBAYM
              AkJFMRAwDgYDVQQKDAdFUEFTT3JnMSYwJAYDVQQLDB1UZWNobmljYWwgQ2VudGVyIG9mIEV4
              cGVydGlzZTEfMB0GA1UEAwwWRVBBUyBQcm90b2NvbHMgVGVzdCBDQTAqGBMyMDEzMDQxODEw
              MTgyMyswMTAwGBMyMDE4MTAwMTE4MjAwNSswMTAwMHgxCzAJBgNVBAYMAkZSMRAwDgYDVQQK
              DAdFUEFTT3JnMSYwJAYDVQQLDB1UZWNobmljYWwgQ2VudGVyIG9mIEV4cGVydGlzZTEvMC0G
              A1UEAwwmRVBBUyBQcm90b2NvbCBUZXN0IEhvc3QgS2V5IEVuY3J5cHRpb24wggGiMA0GCSqG
              SIb3DQEBAQUAA4IBjwAwggGKAoIBgQDXLM9j+y+GahjyGdyRkxZJX/ZskG+QTXsmZSXDf6vn
              1O2Z6gQkM22ZsLeXneF2TnzRa2S5upVGELysu2z9pMuQaqdb7Vi5oANxUlQesdw90LYhTrMb
              6XpPkQc0Et4EIhb6j4JtJMfy0wXUv2NGW/iZ3G8HP/aqM46kTba+UaY1jKo8y4Uo5YtVVA7S
              IyUjMzPT1tK4LteljUmfRF/4NcPr1bUVN5p8K1tB0189/VoaLWFJEDj90Z4Y72eP15SHKsyL
              gSmvoNAvzW5K3pGE1f7COGRBKTsWu3a44uT46AJ2NmhVqIDg76xEnnYSTEv3/yuhXmdLYqVj
              fSZgCqOgE+FTDhH0v5hOUz9SCi50vYJt1QfCg9L1Y8IoSOBdhNK30iIfS2O1Z5fmr7Ql1Wfl
              +Rbjq04sSG7IFIlGnBfaLfr3q0lu58JOQ5Uf/igAa/+W4tFYOKxyUvPUXo/r7w9+75dP/go4
              w4kmz6BoMZjKj9CMiyQnuRoLFveacYbefaud/z0CAwEAAaMPMA0wCwYDVR0PBAQDAgUgMA0G
              CSqGSIb3DQEBCwUAA4ICAQAm7V9OEVqeLRDwezXRDzXYvTu0DUgeXw0uCMgCQdcAArpccwdJ
              HOKJU8tw1J2F0g0Luv29xATvt67dK16Skup2hHg+AtyYlVz7HZQXGeHkj/g/EXQQJDWzUlnn
              UJ+Ptnww3b7ntfVArYkANdYEuY0vCBTnj4+d6dS3evcm22Z8yvcKF1r4f3FpecqHg6gkfjzz
              a9jcMW/h1jGiSJYlPRJCrmWePqFaguc8SylkV69fCIsA9u9Rcw7l5Pqbr27Y5Mw08PuQ/0RC
              1FXzYZpQWcqC3RXLQBMC5w8SS95tUUFW+0Ld5q2mIO8tJ7fyGJtPyrn0SH2ibtRBjwDqTHqJ
              MI6siOWGWUP5Xwh6b7d0m9t4Pirij/fEEK3JNfQWWPNs2Q8syJWifbWtHvFHqmBjSmWRw0Os
              f/lcbX18uI67NhaR/aWGVR1vDK1/5fA3RgNQ5dCmUNYn6wwbUxWwSSQUaEIwu6I51cq5iUIH
              natPDLvOstiB0P/osuGduPlK6dmbrGvixI5f5F3uwv/o+vUrQyVrxQ4X8M7xq4uGlPw0k2J8
              8oUig7JRdt2v7o+6SfQ00rfxvK95zLPq0V86bRGTntxAY1LfamjxIBgxztD+IF4fOBX0bgHm
              5fV5jeLvt89u/leLozrtuz7ZxO856l6aaJnOANtsiSJFCqGCJ1SdtD8WQw==
            </KeyNcphrmntCert>
          </Actn>
        </Cntt>
      </DataSet>
</MgmtPlan>
<SctyTrlr>
  <CnttTp>SIGN</CnttTp>
  <SgndData>
    <DgstAlgo>
      <Algo>HS25</Algo>
    </DgstAlgo>
    <NcpsltdCntt>
      <CnttTp>DATA</CnttTp>
    </NcpsltdCntt>
    <Cert>
      MIIE/zCCAuegAwIBAgIKKrxA9NSC9evJdTANBgkqhkiG9w0BAQsFADBoMQswCQYDVQQGDAJCRTEQMA
      4GA1UECgwHRVBBU09yZzEmMCQGA1UECwwdVGVjaG5pY2FsIENlbnRlciBvZiBFeHBlcnRpc2UxHzAd
      BgNVBAMMFkVQQVMgUHJvdG9jb2xzIFRlc3QgQ0EwKhgTMjAxMzA0MTgxMDA2NDYrMDEwMBgTMjAxOD
      EwMDExODIwMDUrMDEwMDB4MQswCQYDVQQGDAJGUjEQMA4GA1UECgwHRVBBU09yZzEmMCQGA1UECwwd
      VGVjaG5pY2FsIENlbnRlciBvZiBFeHBlcnRpc2UxLzAtBgNVBAMMJkVQQVMgUHJvdG9jb2wgVGVzdC
      BIb3N0IEF1dGhlbnRpY2F0aW9uMIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAvQlYmPmB
      uvQr4g4ZM5s5bFliZpC985bSDFA8pXxoivQeUFUs8bndxBFiCd0AwmtnP37e59DKbcLaqf8vjDqGC4
      +DWuYNngV+3fFiX6xVoQKDf8HH74wKbBN8WXOXKrxA9NSC9evJdU+WS27s7b5m22KtDaezjgWRdWLo
      md9xfSdFdpO0Hnvyy6mIVa4sl95LSP2BKlINbTVgEPboNV7JjbowR/LAzc2b5lUnfz7WmniN2ApqEr
      yj1MfwhmK5nT9wqVSNeAS15KKROj7AJSW+Y57X2bmGVWxZMmdWQvzE5lnYKKlMVUSuu8VEbua5agSg
      GFRwKW38L/unPUB0kwlo3YEOQ9V03XvmZImdpuSOtLO1kOLKqXx1AVxzUJOtYuP9eRq1cY8foQ==
    </Cert>
    <Sgnr>
      <SgnrId>
        <IssrAndSrlNb>
          <Issr>
            <RltvDstngshdNm>
              <AttrTp>CATT</AttrTp>
              <AttrVal>BE</AttrVal>
            </RltvDstngshdNm>
            <RltvDstngshdNm>
              <AttrTp>OATT</AttrTp>
              <AttrVal>EPASOrg</AttrVal>
            </RltvDstngshdNm>
            <RltvDstngshdNm>
              <AttrTp>OUAT</AttrTp>
              <AttrVal>Technical Center of Expertise</AttrVal>
```

```
                  </RltvDstngshdNm>
                  <RltvDstngshdNm>
                     <AttrTp>CNAT</AttrTp>
                     <AttrVal>EPAS Protocols Test CA</AttrVal>
                  </RltvDstngshdNm>
               </Issr>
               <SrlNb>KrxA9NSC9evJdQ==</SrlNb>
            </IssrAndSrlNb>
         </SgnrId>
            <DgstAlgo>
               <Algo>HS25</Algo>
            </DgstAlgo>
            <SgntrAlgo>
               <Algo>ERS2</Algo>
            </SgntrAlgo>
            <Sgntr>
               gR4rOHWF7dSRyBt5zv/xknqVc6aZTRnI74gSvue5eeiDi9rKlFtbn0agGjNYK2PlahZGHxowT+
               ZMK0dyr8deCDTEX3bfM4KDjk7h+pHtlTwu8+cpe7FBr7xGFJ3YWkoquM+zNXg/gBuGkwrFza7B
               Gz8xX75/6eNvK0ovvoJhu5gWdiiidedD28aHUO18NEo7AfDhVx+RVk41JBBDn6lUslh8IhY3KM
               vTu93RICqDG/LIEsvoUGDlqmAF3mAxjXCxqqUkAyUDSJ+SaNrOxMbBqPpQVDMYDgd2F895mFHm
               KqItC2R8rWeKaxCtAb33FngggfqZwT2v9gZG7ax6jZQpD3sv+eOcsmt/6tbS6WYw3hTmIKe5tf
               XLuQGtgRcx408lx3NwHcLFN/h0eWT38FkqmaxurS45CEHOTOAhGkdmoWLSsBS0ah4cWrxBNgGn
               B5eheMWwQK10tLMdTN7Rt5as5zS//jwzsKJ5CXH4JP/An60oYCixRlNdX81IYOd/nwHc
            </Sgntr>
      </Sgnr>
   </SgndData>
 </SctyTrlr>
 </MgmtPlanRplcmnt>
</Document>
```

1.4.5 Status Report to Request a Key Download

To perform the action of the Management Plan, the POI requests the Security Parameters sending the *StatusReport* message containing the session key to encrypt the keys to download.

The POI generates a triple DES 112 bits session key (SK) to encrypt the key encryption key, denoted KEK:

```
0000  AE EF 80 98 A7 3D E9 D6 5B BF 26 64 58 04 02 16  |.....=..[.&dX...|
```

The POI generate the following seed:

```
0000  3F AE 5D 13 77 C7 30 7D 60 D3 9B 6C 6F 3B 93 3D  |?.].w.0}`..lo;.=|
0010  01 89 95 5D 64 DF 4C 67 B6 3B F6 08 F3 F2 84 1C  |...]d.Lg.;......|
```

With the previous seed, the OAEP encryption of this session key Enc[$K_{TM\text{-}Enc}$](SK) is :

```
0000: 0E 8E 47 09 FA 83 A3 2B 80 63 5B D7 D0 F7 F8 B9  |  G    + c[     |
0010: EE A8 14 E9 D2 B7 7A 34 95 84 F5 24 DB DF 60 76  |      z4   $  `v|
0020: 4B 16 CE 42 71 5F 01 D7 49 FC B4 EF B2 51 77 11  |K  Bq_  I    Qw |
0030: A4 9D FD 6D 6F 8E 81 87 51 9C 8F A7 B7 FF 92 8E  |   mo   Q       |
0040: C1 78 3E D7 07 DB C7 D5 79 BC 08 9A 6E AA 87 6C  | x>     y   n  l|
0050: DD 06 16 E9 32 2C 0A CF 43 18 B4 2B 58 35 DD 5B  |    2,  C  +X5 [|
0060: 2C 2F FA E5 46 26 4D 61 5F 79 88 E0 D4 DC 53 F6  |,/  F&Ma_y    S |
0070: 20 4B D6 35 B1 B7 24 F0 51 F8 46 93 9E D1 13 B1  | K 5  $ Q F     |
0080: A3 90 EE 6B 02 E1 14 12 BB D2 4D 5F 73 65 32 05  |   k      M_se2 |
0090: 9D 54 E4 8C 9A 67 39 C1 CE 5D 48 B0 A6 90 67 EA  | T   g9  ]H   g |
00A0: 76 24 CF A4 4B D8 BD 7E FD 2D 3E BE 58 76 39 89  |v$  K  ~ -> Xv9 |
00B0: C7 4A CA 5B 38 F3 8D D0 C8 EE FF EE 7F EC A8 A5  | J [8           |
00C0: 47 5E 0E 3D 32 98 00 7A C6 E9 44 2A 6D D3 1B 7D  |G^ =2  z  D*m  }|
00D0: 3C 1B AE F5 A6 DE B3 37 AA FF A4 83 6E 8D 09 1E  |<      7    n   |
00E0: EF 98 2A EC C0 BA 5F B0 5E 48 6B 51 DA 82 02 64  |  *    _ ^HkQ   d|
00F0: 20 26 1A 8F 05 5C 40 B4 F3 60 8D 7B 07 FF C2 0C  | &   \@  ` {    |
0100: 71 69 4A 9E DC 2A 54 8B 72 CA C2 DC 38 2D B1 AF  |qiJ  *T r   8-  |
0110: F7 E0 F6 1F F9 06 86 01 CA 90 3A 1F 2C 59 8F FF  |          : ,Y  |
0120: D8 86 EC 23 A9 25 F6 F3 4E 49 BE AC 43 83 6D 76  |   # %  NI  C mv|
0130: EF C8 B3 88 F4 F2 CB E6 45 AD 10 14 C3 29 E8 09  |        E    )  |
0140: 2C A3 71 7C 88 4D A8 6A 7F A5 8E 8D 96 DB 31 57  |, q| M j      1W|
0150: 85 1A 56 98 F5 5D BA 0C 4D 26 21 A0 E1 58 AE 06  |  V  ]  M&!  X  |
0160: 87 86 95 31 AF 1C 6B 1F E4 CA 99 B1 C5 D2 1E 11  |   1  k         |
0170: 69 23 B9 09 42 7D 5B 94 96 B5 82 C6 2D 15 BA 69  |i#  B}[     -  i|
```

The POI generates the triple DES 112 bits KEK key:

```
0000  A7 5D 20 F7 04 51 75 45 3E 29 25 9D 3B 08 A7 2A  |.] ..QuE>)%.;..*|
```

Applying the padding process, the hexadecimal byte `80` is appended, followed by 7 null bytes:

```
0000  A7 5D 20 F7 04 51 75 45 3E 29 25 9D 3B 08 A7 2A  |.] ..QuE>)%.;..*|
0010  80 00 00 00 00 00 00 00                          |........        |
```

Using the Initialisation Vector value `A27BB46D1C306E09`, the Triple DES CBC encryption by SK of the padded KEK provides the values below:

```
0000  9F 04 15 02 7B 61 F4 6C 85 1D A5 35 96 89 4E 25  |....{a.l...5..N%|
0010  AD 20 A8 F1 EE 6B A1 38                          |. ...k.8        |
```

1487 The *StatusReport* message containing the header and the body presented in the table below:

Message Item	*Value*
Header	
DownloadTransfer	False
FormatVersion	6.0
ExchangeIdentification	002
CreationDateTime	2013-12-06:13:53:53.00+02:00
InitiatingParty	
Identification	66000001
Type	OriginationgPOI
Issuer	MasterTerminalManager
RecipientParty	
Identification	epas-keyDownload-TM1
Type	MasterTerminalManager
StatusReport	
POIIdentification	
Identification	66000001
Type	OriginationgPOI
Issuer	MasterTerminalManager
TerminalManagerdentification	
Identification	epas-keyDownload-TM1
Type	MasterTerminalManager
DataSet	
Identification	
Type	StatusReport
CreationDateTime	2013-12-06:13:53:53.00+02:00
Content	
POIComponent	
Type	Terminal
Identification	
ItemNumber	1
ProviderIdentification	EPASVendor001
Identification	Counter Top E41
SerialNumber	7825410759
POIComponent	
Type	PaymentApplication
Identification	
ItemNumber	1.1
ProviderIdentification	EPASVendor001
Status	
VersionNumber	1.01
StandardCompliance	
Identification	SEPA-FAST
VersionNumber	3.0
Issuer	CIR
AttendanceContext	Attended
POIDateTime	2013-12-06:13:53:53.00+02:00
DataSetRequired	
Identification	
Name	epas-acquirer-TM1-TIK
Type	SecurityParameters

Version	20131206135352
CreationDateTime	2013-12-06T13:53:52.00+02:00
POIChallenge	D1377C7307D60D39B6C6F3B933D0089955D64DF4C67B63BF608F3F2841C77051
TMChallenge	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SessionKey	
Identification	Key Encryption Key KEK
Version	01
Type	DES112
Function	KeyExport
KeyValue	
EnvelopedData	
Recipient	
KeyTransport	
Version	0
RecipientIdentification	
IssuerAndSerial-Number	
Issuer	
Relative-Distinguished-Name	
AtributeType	CountryName
AttributeName	BE
Relative-Distinguished-Name	
AtributeType	OrganisationName
AttributeName	EPASOrg
Relative-Distinguished-Name	
AtributeType	OrganisationUnitName
AttributeName	Technical Center of Expertise
Relative-Distinguished-Name	
AtributeType	CommonName
AttributeName	EPAS Protocols Test CA
SerialNumber	7895CA35014C3D2F1E11B10D
KeyEncryptionAlgorithm	
Algorithm	RSAES-OAEP
Parameter	
DigestAlgorithm	SHA256
MaskGenerator-Algorithm	
Algorithm	MGF1
Parameter	
DigestAlgorithm	SHA256

EncryptedKey	0E8E4709FA83A32B80635BD7D0F7F8B9EEA814E9D2B77A34958 4F524DBDF60764B16CE42715F01D749FCB4EFB2517711A49DFD 6D6F8E8187519C8FA7B7FF928EC1783ED707DBC7D579BC089A6 EAA876CDD0616E9322C0ACF4318B42B5835DD5B2C2FFAE54626 4D615F7988E0D4DC53F6204BD635B1B724F051F846939ED113B 1A390EE6B02E11412BBD24D5F736532059D54E48C9A6739C1CE 5D48B0A69067EA7624CFA44BD8BD7EFD2D3EBE58763989C74AC A5B38F38DD0C8EEFFEE7FECA8A5475E0E3D3298007AC6E9442A 6DD31B7D3C1BAEF5A6DEB337AAFFA4836E8D091EEF982AECC0B A5FB05E486B51DA82026420261A8F055C40B4F3608D7B07FFC2 0C71694A9EDC2A548B72CAC2DC382DB1AFF7E0F61FF9068601C A903A1F2C598FFFD886EC23A925F6F34E49BEAC43836D76EFC8 B388F4F2CBE645AD1014C329E8092CA3717C884DA86A7FA58E8 D96DB3157851A5698F55DBA0C4D2621A0E158AE0687869531AF 1C6B1FE4CA99B1C5D21E116923B909427D5B9496B582C62D15B A69
EncryptedContent	
ContentType	PlainData
ContentEncryptionAlgorithm	
Algorithm	DES112CBC
Parameter	
InitialisationVector	A27BB46D1C306E09
EncryptedData	9F0415027B61F46C851DA53596894E25AD20A8F1EE6BA138

Once unnecessary spaces and carriage returns are removed, the XML encoded *StatusReport* message body is:

```
0000  3C 53 74 73 52 70 74 3E 3C 50 4F 49 49 64 3E 3C  |<StsRpt><POIId><|
0010  49 64 3E 36 36 30 30 30 30 30 31 3C 2F 49 64 3E  |Id>66000001</Id>|
0020  3C 54 70 3E 4F 50 4F 49 3C 2F 54 70 3E 3C 49 73  |<Tp>OPOI</Tp><Is|
0030  73 72 3E 4D 54 4D 47 3C 2F 49 73 73 72 3E 3C 2F  |sr>MTMG</Issr></|
0040  50 4F 49 49 64 3E 3C 54 65 72 6D 6E 6C 4D 67 72  |POIId><TermnlMgr|
0050  49 64 3E 3C 49 64 3E 65 70 61 73 2D 6B 65 79 44  |Id><Id>epas-keyD|
0060  6F 77 6E 6C 6F 61 64 2D 54 4D 31 3C 2F 49 64 3E  |ownload-TM1</Id>|
0070  3C 54 70 3E 4D 54 4D 47 3C 2F 54 70 3E 3C 2F 54  |<Tp>MTMG</Tp></T|
0080  65 72 6D 6E 6C 4D 67 72 49 64 3E 3C 44 61 74 61  |ermnlMgrId><Data|
0090  53 65 74 3E 3C 49 64 3E 3C 54 70 3E 53 54 52 50  |Set><Id><Tp>STRP|
00A0  3C 2F 54 70 3E 3C 43 72 65 44 74 54 6D 3E 32 30  |</Tp><CreDtTm>20|
00B0  31 33 2D 31 32 2D 30 36 54 31 33 3A 35 33 3A 35  |13-12-06T13:53:5|
00C0  33 2E 30 30 2B 30 32 3A 30 30 3C 2F 43 72 65 44  |3.00+02:00</CreD|
00D0  74 54 6D 3E 3C 2F 49 64 3E 3C 43 6E 74 74 3E 3C  |tTm></Id><Cntt><|
00E0  50 4F 49 43 6D 70 6E 74 3E 3C 54 70 3E 54 45 52  |POICmpnt><Tp>TER|
00F0  4D 3C 2F 54 70 3E 3C 49 64 3E 3C 49 74 6D 4E 62  |M</Tp><Id><ItmNb|
0100  3E 31 3C 2F 49 74 6D 4E 62 3E 3C 50 72 76 64 72  |>1</ItmNb><Prvdr|
0110  49 64 3E 45 50 41 53 56 65 6E 64 6F 72 30 30 31  |Id>EPASVendor001|
0120  3C 2F 50 72 76 64 72 49 64 3E 3C 49 64 3E 43 6F  |</PrvdrId><Id>Co|
0130  75 6E 74 65 72 20 54 6F 70 20 45 34 31 3C 2F 49  |unter Top E41</I|
0140  64 3E 3C 53 72 6C 4E 62 3E 37 38 32 35 34 31 30  |d><SrlNb>7825410|
0150  37 35 39 3C 2F 53 72 6C 4E 62 3E 3C 2F 49 64 3E  |759</SrlNb></Id>|
0160  3C 2F 50 4F 49 43 6D 70 6E 74 3E 3C 50 4F 49 43  |</POICmpnt><POIC|
0170  6D 70 6E 74 3E 3C 54 70 3E 41 50 4C 49 3C 2F 54  |mpnt><Tp>APLI</T|
0180  70 3E 3C 49 64 3E 3C 49 74 6D 4E 62 3E 31 2E 31  |p><Id><ItmNb>1.1|
0190  3C 2F 49 74 6D 4E 62 3E 3C 50 72 76 64 72 49 64  |</ItmNb><PrvdrId|
01A0  3E 45 50 41 53 56 65 6E 64 6F 72 30 30 31 3C 2F  |>EPASVendor001</|
01B0  50 72 76 64 72 49 64 3E 3C 2F 49 64 3E 3C 53 74  |PrvdrId></Id><St|
01C0  73 3E 3C 56 72 73 6E 4E 62 3E 31 2E 30 31 3C 2F  |s><VrsnNb>1.01</|
```

```
01D0  56 72 73 6E 4E 62 3E 3C 2F 53 74 73 3E 3C 53 74  |VrsnNb></Sts><St|
01E0  64 43 6D 70 6C 63 3E 3C 49 64 3E 53 45 50 41 2D  |dCmplc><Id>SEPA-|
01F0  46 41 53 54 3C 2F 49 64 3E 3C 56 72 73 6E 3E 33  |FAST</Id><Vrsn>3|
0200  2E 30 3C 2F 56 72 73 6E 3E 3C 49 73 73 72 3E 43  |.0</Vrsn><Issr>C|
0210  49 52 3C 2F 49 73 73 72 3E 3C 2F 53 74 64 43 6D  |IR</Issr></StdCm|
0220  70 6C 63 3E 3C 2F 50 4F 49 43 6D 70 6E 74 3E 3C  |plc></POICmpnt><|
0230  41 74 74 6E 64 6E 63 43 6E 74 78 74 3E 41 54 54  |AttndncCntxt>ATT|
0240  44 3C 2F 41 74 74 6E 64 6E 63 43 6E 74 78 74 3E  |D</AttndncCntxt>|
0250  3C 50 4F 49 44 74 54 6D 3E 32 30 31 33 2D 31 32  |<POIDtTm>2013-12|
0260  2D 30 36 54 31 33 3A 35 33 3A 35 33 2E 30 30 2B  |-06T13:53:53.00+|
0270  30 32 3A 30 30 3C 2F 50 4F 49 44 74 54 6D 3E 3C  |02:00</POIDtTm><|
0280  44 61 74 61 53 65 74 52 65 71 72 64 3E 3C 49 64  |DataSetReqrd><Id|
0290  3E 3C 4E 6D 3E 65 70 61 73 2D 61 63 71 75 69 72  |><Nm>epas-acquir|
02A0  65 72 2D 54 4D 31 2D 54 49 4B 3C 2F 4E 6D 3E 3C  |er-TM1-TIK</Nm><|
02B0  54 70 3E 53 43 50 52 3C 2F 54 70 3E 3C 56 72 73  |Tp>SCPR</Tp><Vrs|
02C0  6E 3E 32 30 31 33 31 32 30 36 31 33 35 33 35 32  |n>20131206135352|
02D0  3C 2F 56 72 73 6E 3E 3C 43 72 65 44 74 54 6D 3E  |</Vrsn><CreDtTm>|
02E0  32 30 31 33 2D 31 32 2D 30 36 54 31 33 3A 35 33  |2013-12-06T13:53|
02F0  3A 35 32 2E 30 30 2B 30 32 3A 30 30 3C 2F 43 72  |:52.00+02:00</Cr|
0300  65 44 74 54 6D 3E 3C 2F 49 64 3E 3C 50 4F 49 43  |eDtTm></Id><POIC|
0310  68 6C 6C 6E 67 3E 30 54 64 38 63 77 66 57 44 54  |hllng>0Td8cwfWDT|
0320  6D 32 78 76 4F 35 4D 39 41 49 6D 56 58 57 54 66  |m2xvO5M9AImVXWTf|
0330  54 47 65 32 4F 2F 59 49 38 2F 4B 45 48 48 63 46  |TGe2O/YI8/KEHHcF|
0340  45 3D 3C 2F 50 4F 49 43 68 6C 6C 6E 67 3E 3C 54  |E=</POIChllng><T|
0350  4D 43 68 6C 6C 6E 67 3E 34 37 44 45 51 70 6A 38  |MChllng>47DEQpj8|
0360  48 42 53 61 2B 2F 54 49 6D 57 2B 35 4A 43 65 75  |HBSa+/TImW+5JCeu|
0370  51 65 52 6B 6D 35 4E 4D 70 4A 57 5A 47 33 68 53  |QeRkm5NMpJWZG3hS|
0380  75 46 55 3D 3C 2F 54 4D 43 68 6C 6C 6E 67 3E 3C  |uFU=</TMChllng><|
0390  53 73 6E 4B 65 79 3E 3C 49 64 3E 4B 65 79 20 45  |SsnKey><Id>Key E|
03A0  6E 63 72 79 70 74 69 6F 6E 20 4B 65 79 20 4B 45  |ncryption Key KE|
03B0  4B 3C 2F 49 64 3E 3C 56 72 73 6E 3E 30 31 3C 2F  |K</Id><Vrsn>01</|
03C0  56 72 73 6E 3E 3C 54 70 3E 45 44 45 33 3C 2F 54  |Vrsn><Tp>EDE3</T|
03D0  70 3E 3C 46 63 74 6E 3E 4B 45 59 58 3C 2F 46 63  |p><Fctn>KEYX</Fc|
03E0  74 6E 3E 3C 4B 65 79 56 61 6C 3E 3C 43 6E 74 74  |tn><KeyVal><Cntt|
03F0  54 70 3E 45 56 4C 50 3C 2F 43 6E 74 74 54 70 3E  |Tp>EVLP</CnttTp>|
0400  3C 45 6E 76 6C 70 64 44 61 74 61 3E 3C 52 63 70  |<EnvlpdData><Rcp|
0410  74 3E 3C 4B 65 79 54 72 6E 73 70 72 74 3E 3C 56  |t><KeyTrnsprt><V|
0420  72 73 6E 3E 30 3C 2F 56 72 73 6E 3E 3C 52 63 70  |rsn>0</Vrsn><Rcp|
0430  74 49 64 3E 3C 49 73 73 72 41 6E 64 53 72 6C 4E  |tId><IssrAndSrlN|
0440  62 3E 3C 49 73 73 72 3E 3C 52 6C 74 76 44 73 74  |b><Issr><RltvDst|
0450  6E 67 73 68 64 4E 6D 3E 3C 41 74 74 72 54 70 3E  |ngshdNm><AttrTp>|
0460  43 41 54 54 3C 2F 41 74 74 72 54 70 3E 3C 41 74  |CATT</AttrTp><At|
0470  74 72 56 61 6C 3E 42 45 3C 2F 41 74 74 72 56 61  |trVal>BE</AttrVa|
0480  6C 3E 3C 2F 52 6C 74 76 44 73 74 6E 67 73 68 64  |l></RltvDstngshd|
0490  4E 6D 3E 3C 52 6C 74 76 44 73 74 6E 67 73 68 64  |Nm><RltvDstngshd|
04A0  4E 6D 3E 3C 41 74 74 72 54 70 3E 4F 41 54 54 3C  |Nm><AttrTp>OATT<|
04B0  2F 41 74 74 72 54 70 3E 3C 41 74 74 72 56 61 6C  |/AttrTp><AttrVal|
04C0  3E 45 50 41 53 4F 72 67 3C 2F 41 74 74 72 56 61  |>EPASOrg</AttrVa|
04D0  6C 3E 3C 2F 52 6C 74 76 44 73 74 6E 67 73 68 64  |l></RltvDstngshd|
04E0  4E 6D 3E 3C 52 6C 74 76 44 73 74 6E 67 73 68 64  |Nm><RltvDstngshd|
04F0  4E 6D 3E 3C 41 74 74 72 54 70 3E 4F 55 41 54 3C  |Nm><AttrTp>OUAT<|
0500  2F 41 74 74 72 54 70 3E 3C 41 74 74 72 56 61 6C  |/AttrTp><AttrVal|
0510  3E 54 65 63 68 6E 69 63 61 6C 20 43 65 6E 74 65  |>Technical Cente|
0520  72 20 6F 66 20 45 78 70 65 72 74 69 73 65 3C 2F  |r of Expertise</|
```

```
0530  41 74 74 72 56 61 6C 3E 3C 2F 52 6C 74 76 44 73  |AttrVal></RltvDs|
0540  74 6E 67 73 68 64 4E 6D 3E 3C 52 6C 74 76 44 73  |tngshdNm><RltvDs|
0550  74 6E 67 73 68 64 4E 6D 3E 3C 41 74 74 72 54 70  |tngshdNm><AttrTp|
0560  3E 43 4E 41 54 3C 2F 41 74 74 72 54 70 3E 3C 41  |>CNAT</AttrTp><A|
0570  74 74 72 56 61 6C 3E 45 50 41 53 20 50 72 6F 74  |ttrVal>EPAS Prot|
0580  6F 63 6F 6C 73 20 54 65 73 74 20 43 41 3C 2F 41  |ocols Test CA</A|
0590  74 74 72 56 61 6C 3E 3C 2F 52 6C 74 76 44 73 74  |ttrVal></RltvDst|
05A0  6E 67 73 68 64 4E 6D 3E 3C 2F 49 73 73 72 3E 3C  |ngshdNm></Issr><|
05B0  53 72 6C 4E 62 3E 65 4A 58 4B 4E 51 46 4D 50 53  |SrlNb>eJXKNQFMPS|
05C0  38 65 45 62 45 4E 3C 2F 53 72 6C 4E 62 3E 3C 2F  |8eEbEN</SrlNb></|
05D0  49 73 73 72 41 6E 64 53 72 6C 4E 62 3E 3C 2F 52  |IssrAndSrlNb></R|
05E0  63 70 74 49 64 3E 3C 4B 65 79 4E 63 72 70 74 6E  |cptId><KeyNcrptn|
05F0  41 6C 67 6F 3E 3C 41 6C 67 6F 3E 52 53 41 4F 3C  |Algo><Algo>RSAO<|
0600  2F 41 6C 67 6F 3E 3C 50 61 72 61 6D 3E 3C 44 67  |/Algo><Param><Dg|
0610  73 74 41 6C 67 6F 3E 48 53 32 35 3C 2F 44 67 73  |stAlgo>HS25</Dgs|
0620  74 41 6C 67 6F 3E 3C 4D 73 6B 47 6E 72 74 72 41  |tAlgo><MskGnrtrA|
0630  6C 67 6F 3E 3C 41 6C 67 6F 3E 4D 47 46 31 3C 2F  |lgo><Algo>MGF1</|
0640  41 6C 67 6F 3E 3C 50 61 72 61 6D 3E 3C 44 67 73  |Algo><Param><Dgs|
0650  74 41 6C 67 6F 3E 48 53 32 35 3C 2F 44 67 73 74  |tAlgo>HS25</Dgst|
0660  41 6C 67 6F 3E 3C 2F 50 61 72 61 6D 3E 3C 2F 4D  |Algo></Param></M|
0670  73 6B 47 6E 72 74 72 41 6C 67 6F 3E 3C 2F 50 61  |skGnrtrAlgo></Pa|
0680  72 61 6D 3E 3C 2F 4B 65 79 4E 63 72 70 74 6E 41  |ram></KeyNcrptnA|
0690  6C 67 6F 3E 3C 4E 63 72 70 74 64 4B 65 79 3E 44  |lgo><NcrptdKey>D|
06A0  6F 35 48 43 66 71 44 6F 79 75 41 59 31 76 58 30  |o5HCfqDoyuAY1vX0|
06B0  50 66 34 75 65 36 6F 46 4F 6E 53 74 33 6F 30 6C  |Pf4ue6oFOnSt3o0l|
06C0  59 54 31 4A 4E 76 66 59 48 5A 4C 46 73 35 43 63  |YT1JNvfYHZLFs5Cc|
06D0  56 38 42 31 30 6E 38 74 4F 2B 79 55 58 63 52 70  |V8B10n8tO+yUXcRp|
06E0  4A 33 39 62 57 2B 4F 67 59 64 52 6E 49 2B 6E 74  |J39bW+OgYdRnI+nt|
06F0  2F 2B 53 6A 73 46 34 50 74 63 48 32 38 66 56 65  |/+SjsF4PtcH28fVe|
0700  62 77 49 6D 6D 36 71 68 32 7A 64 42 68 62 70 4D  |bwImm6qh2zdBhbpM|
0710  69 77 4B 7A 30 4D 59 74 43 74 59 4E 64 31 62 4C  |iwKz0MYtCtYNd1bL|
0720  43 2F 36 35 55 59 6D 54 57 46 66 65 59 6A 67 31  |C/65UYmTWFfeYjg1|
0730  4E 78 54 39 69 42 4C 31 6A 57 78 74 79 54 77 55  |NxT9iBL1jWxtyTwU|
0740  66 68 47 6B 35 37 52 45 37 47 6A 6B 4F 35 72 41  |fhGk57RE7GjkO5rA|
0750  75 45 55 45 72 76 53 54 56 39 7A 5A 54 49 46 6E  |uEUErvSTV9zZTIFn|
0760  56 54 6B 6A 4A 70 6E 4F 63 48 4F 58 55 69 77 70  |VTkjJpnOcHOXUiwp|
0770  70 42 6E 36 6E 59 6B 7A 36 52 4C 32 4C 31 2B 2F  |pBn6nYkz6RL2L1+/|
0780  53 30 2B 76 6C 68 32 4F 59 6E 48 53 73 70 62 4F  |S0+vlh2OYnHSspbO|
0790  50 4F 4E 30 4D 6A 75 2F 2B 35 2F 37 4B 69 6C 52  |PON0Mju/+5/7KilR|
07A0  31 34 4F 50 54 4B 59 41 48 72 47 36 55 51 71 62  |14OPTKYAHrG6UQqb|
07B0  64 4D 62 66 54 77 62 72 76 57 6D 33 72 4D 33 71  |dMbfTwbrvWm3rM3q|
07C0  76 2B 6B 67 32 36 4E 43 52 37 76 6D 43 72 73 77  |v+kg26NCR7vmCrsw|
07D0  4C 70 66 73 46 35 49 61 31 48 61 67 67 4A 6B 49  |LpfsF5Ia1HaggJkI|
07E0  43 59 61 6A 77 56 63 51 4C 54 7A 59 49 31 37 42  |CYajwVcQLTzYI17B|
07F0  2F 2F 43 44 48 46 70 53 70 37 63 4B 6C 53 4C 63  |//CDHFpSp7cKlSLc|
0800  73 72 43 33 44 67 74 73 61 2F 33 34 50 59 66 2B  |srC3Dgtsa/34PYf+|
0810  51 61 47 41 63 71 51 4F 68 38 73 57 59 2F 2F 32  |QaGAcqQOh8sWY//2|
0820  49 62 73 49 36 6B 6C 39 76 4E 4F 53 62 36 73 51  |IbsI6kl9vNOSb6sQ|
0830  34 4E 74 64 75 2F 49 73 34 6A 30 38 73 76 6D 52  |4Ntdu/Is4j08svmR|
0840  61 30 51 46 4D 4D 70 36 41 6B 73 6F 33 46 38 69  |a0QFMMp6Akso3F8i|
0850  45 32 6F 61 6E 2B 6C 6A 6F 32 57 32 7A 46 58 68  |E2oan+ljo2W2zFXh|
0860  52 70 57 6D 50 56 64 75 67 78 4E 4A 69 47 67 34  |RpWmPVdugxNJiGg4|
0870  56 69 75 42 6F 65 47 6C 54 47 76 48 47 73 66 35  |ViuBoeGlTGvHGsf5|
0880  4D 71 5A 73 63 58 53 48 68 46 70 49 37 6B 4A 51  |MqZscXSHhFpI7kJQ|
```

```
0890  6E 31 62 6C 4A 61 31 67 73 59 74 46 62 70 70 3C  |n1blJa1gsYtFbpp<|
08A0  2F 4E 63 72 70 74 64 4B 65 79 3E 3C 2F 4B 65 79  |/NcrptdKey></Key|
08B0  54 72 6E 73 70 72 74 3E 3C 2F 52 63 70 74 3E 3C  |Trnsprt></Rcpt><|
08C0  4E 63 72 70 74 64 43 6E 74 74 3E 3C 43 6E 74 74  |NcrptdCntt><Cntt|
08D0  54 70 3E 44 41 54 41 3C 2F 43 6E 74 74 54 70 3E  |Tp>DATA</CnttTp>|
08E0  3C 43 6E 74 74 4E 63 72 70 74 6E 41 6C 67 6F 3E  |<CnttNcrptnAlgo>|
08F0  3C 41 6C 67 6F 3E 45 33 44 43 3C 2F 41 6C 67 6F  |<Algo>E3DC</Algo|
0900  3E 3C 50 61 72 61 6D 3E 3C 49 6E 69 74 6C 73 74  |><Param><Initlst|
0910  6E 56 63 74 72 3E 6F 6E 75 30 62 52 77 77 62 67  |nVctr>onu0bRwwbg|
0920  6B 3D 3C 2F 49 6E 69 74 6C 73 74 6E 56 63 74 72  |k=</InitlstnVctr|
0930  3E 3C 2F 50 61 72 61 6D 3E 3C 2F 43 6E 74 74 4E  |></Param></CnttN|
0940  63 72 70 74 6E 41 6C 67 6F 3E 3C 4E 63 72 70 74  |crptnAlgo><Ncrpt|
0950  64 44 61 74 61 3E 6E 77 51 56 41 6E 74 68 39 47  |dData>nwQVAnth9G|
0960  79 46 48 61 55 31 6C 6F 6C 4F 4A 61 30 67 71 50  |yFHaU1lolOJa0gqP|
0970  48 75 61 36 45 34 3C 2F 4E 63 72 70 74 64 44 61  |Hua6E4</NcrptdDa|
0980  74 61 3E 3C 2F 4E 63 72 70 74 64 43 6E 74 74 3E  |ta></NcrptdCntt>|
0990  3C 2F 45 6E 76 6C 70 64 44 61 74 61 3E 3C 2F 4B  |</EnvlpdData></K|
09A0  65 79 56 61 6C 3E 3C 2F 53 73 6E 4B 65 79 3E 3C  |eyVal></SsnKey><|
09B0  2F 44 61 74 61 53 65 74 52 65 71 72 64 3E 3C 2F  |/DataSetReqrd></|
09C0  43 6E 74 74 3E 3C 2F 44 61 74 61 53 65 74 3E 3C  |Cntt></DataSet><|
09D0  2F 53 74 73 52 70 74 3E                          |/StsRpt>        |
```

The SHA256 digest of the *StatusReport* message body is:

```
0000  08 A6 49 61 C5 4E C2 79 14 C2 2D 9C AE C9 B9 F8  |..Ia.N.y..-.....|
0010  14 F9 1B 39 5A 7F 2C 30 AC 38 04 47 75 31 7D 46  |...9Z.,0.8.Gu1}F|
```

Applying the padding process for the digital signature, the block result is dumped below:

```
0000  00 01 FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0010  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0020  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0030  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0040  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0050  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0060  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0070  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0080  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0090  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
00A0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
00B0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
00C0  FF FF FF FF FF FF FF FF FF FF FF FF 00 30 31 30  |.............010|
00D0  0D 06 09 60 86 48 01 65 03 04 02 01 05 00 04 20  |...`.H.e....... |
00E0  08 A6 49 61 C5 4E C2 79 14 C2 2D 9C AE C9 B9 F8  |..Ia.N.y..-.....|
00F0  14 F9 1B 39 5A 7F 2C 30 AC 38 04 47 75 31 7D 46  |...9Z.,0.8.Gu1}F|
```

After encryption by the private key of $K_{POI\text{-}Sign}$, we have the digital signature of the *StatusReport* message body:

```
0000  52 5E 91 3C D2 62 6D 6D F5 CB 67 85 A3 24 01 D1  |R^.<.bmm..g..$..|
0010  AB 3C 5A 57 C3 B7 1F 10 73 A7 A1 5A C4 12 FF 8D  |.<ZW....s..Z....|
0020  4C 53 4B 3F E4 7C B5 6A 0C 9B C7 2F A2 22 79 D0  |LSK?.|.j.../."y.|
0030  1F 74 76 B5 40 C5 BA BF 48 AE 39 11 4E 5B 67 4B  |.tv.@...H.9.N[gK|
0040  D2 6B F5 46 36 57 FE 16 5B E4 53 D2 BB F5 31 F3  |.k.F6W..[.S...1.|
0050  F2 56 B7 09 B2 8E DF 63 1D AD AD 57 59 3F D4 67  |.V.....c...WY?.g|
0060  18 78 79 30 2D CB 9E 35 FC A7 4C FC 5C E9 2B 6E  |.xy0-..5..L.\.+n|
0070  12 2A E9 3D A5 7A 0B 27 91 D4 5D F3 00 6A DF 72  |.*.=.z.'..]..j.r|
0080  18 37 BB AB CB E8 91 FD 9E B9 BD 11 FA F4 1F 1B  |.7..............|
0090  6F 31 C9 79 67 B5 4B 76 F2 90 42 60 FA E4 51 B0  |o1.yg.Kv..B`..Q.|
00A0  BC 59 6D 60 D0 AF C7 82 AC 0B 89 19 D5 2B 24 A6  |.Ym`.........+$.|
00B0  D7 1C F1 1F EA 08 23 81 FD EB BF EC AE E5 7F CB  |......#.........|
00C0  4B 17 7C 1A B0 F1 6D 62 7D FE CE AF D9 D7 A9 B8  |K.|...mb}.......|
00D0  06 31 E0 C3 3A FA 7D 26 F2 F8 AA 76 AE 46 8A C1  |.1..:.}&...v.F..|
00E0  59 07 F3 F5 F1 D9 BF 03 0F 49 C9 C0 0D C8 6E 10  |Y........I....n.|
00F0  24 60 49 EB C4 85 E1 BA 2B 44 B2 A9 87 60 D7 0E  |$`I.....+D...`..|
```

Inside the *SecurityTrailer*, the *SignedData* CMS data structure is presented in the table below:

Message Item	*Value*
SecurityTrailer	
SignedData	
ContentType	SignedData
DigestAlgorithm	
Algorithm	SHA256
EncapsulatedContent	
ContentType	PlainData

Certificate	308204833082026BA003020102020C2225A8FB00071293D4641C3C300D06092A 864886F70D01010B05003068310B300906035504060C0242453110300E060355 040A0C07455041534F72673126302406035504 0B0C1D546563686E6963616C20 43656E746572206F662045787065727469736531 1F301D06035504030C164550 41532050726F746F636F6C732054657374204341302A181332303133303431 38 3130323534362B303130301813323031383130303131383230303052B30313030 307A310B300906035504060C0246523110300E060355040A0C07455041534F72 673126302406035504 0B0C1D546563686E6963616C2043656E746572206F6620 45787065727469736531 31302F06035504030C28455041532050726F746F636F 6C205465737420436C69656E742041757468656E7469636174696F6E30820122 300D06092A864886F70D01010105000382010F003082010A0282010100C22511 390B85DB3990A27638B850616C18B11BDF78494B48B61F8F8D032225A8FB0007 1293D4641C3CDDE18D47337EB7381AC12976820FF5C0B321E4EDF88C9B8F1627 0E0FC6FAB470449BA70B947139551ABE326686F538C4F7F63A45FF4CB9E66470 00B28B791E1205ADB6ACDC29854698D90ACC3B6C84F0F8C2EFBEE4E3F9844BD7 9AB14C1F22376198C13BEAC560DDC835104176729C7E62FBF4EC350DE4D385C4 8D3EA40A90D7AA5838FAED3E3C760D19BB84D1997077C72331F3ADF050B41DB5 FFD19D129E88C75331DA13264BE4C2F0B0A0AA09F77EED2C801FAD239E8FE5D8 B43F10708FC3D6054B9156C5B55184F1A294DAB8F8267162BE9BB54867020301 0001A30F300D300B0603551D0F040403020780300D06092A864886F70D01010B 05000382020100540DB4CCCA78C5B72EC34D6A55EE7C152ED54409419E0B7BC7 83B8559557C02CCA5E81B6CCA854A36250ADCA0CD55C96F42F019799B5A100C9 72D3F2411CB2676300F1B09E46AE4F293A24CB71EEA5467CB91933713E556FFC C0B558DA344FF4F8AB30A2F803BD97BB568100BAC6B6FAE884F831BF855C4EE8 23FE3BAC3BA2D8B615F62C1C1685B9BC59DFCBE1CFBDFDB29F3773FD46685688 BF656670F5BB9CE56B029E36E7291629DE69FA858367619D8DE4FB9F08608518 85A42894ADC97DCB51D4CEBF9F52083DD511371B157E3D16F93469EED0B7FF01 BC137D5065E266A8EA3C82999EF36263A863ED5FE22A69E4874FDF41A19FA457 B12CF6A52B08F73BD3BD9C2FD13352ECEE4EEF6323826BF72440FC149EBD5891 A8D6D0E5DA50547708525CA4021B51059B52B50E61B176C1F962AA7AC2809934 31DD5BF3D6C146ADBA762B3E6729F17FA639D98D5CBFDCAE556A2FC0B23754E4 91F97BF17A18D842A87F8DE4FBA58B56517213BC59C512D4F0447F0C197B3878 5A457E0A0E7DD44806C4BA16F811B7A25024791ED742E74392C9D4BABA754F09 B61DD8EC2ABBF6737E492BBC37185072AC9EBEA3DEF2FBD56E836B88D0809F96 A4B2ACA1A5B59D198F94990BA4D2A1B50CF64C5E8391D6DCADB58C9E074E608D 7D012309A92FFDCEFD96CDAEA4F6BE5E572A20161C3D6FD838FFAE966BB2C671 E7C836FB369C28
Signer	
SignerIdentification	
IssuerAnd-SerialNumber	
Issuer	
RelativeDistin-guishedName	
AttributeType	CountryName
AttributeValue	BE
RelativeDistin-guishedName	
AttributeType	OrganisationName
AttributeValue	EPASOrg
RelativeDistin-guishedName	
AttributeType	OrganisationUnitName
AttributeValue	Technical Center of Expertise
RelativeDistin-guishedName	
AttributeType	CommonName
AttributeValue	EPAS Protocols Test CA
SerialNumber	2225A8FB00071293D4641C3C
DigestAlgorithm	
Algorithm	SHA256
SignatureAlgorithm	
Algorithm	SHA256WithRSA

Signature	525E913CD2626D6DF5CB6785A32401D1AB3C5A57C3B71F1073A7A15AC412FF8D 4C534B3FE47CB56A0C9BC72FA22279D01F7476B540C5BABF48AE39114E5B674B D26BF5463657FE165BE453D2BBF531F3F256B709B28EDF631DADAD57593FD467 187879302DCB9E35FCA74CFC5CE92B6E122AE93DA57A0B2791D45DF3006ADF72 1837BBABCBE891FD9EB9BD11FAF41F1B6F31C97967B54B76F2904260FAE451B0 BC596D60D0AFC782AC0B8919D52B24A6D71CF11FEA082381FDEBBFECAEE57FCB 4B177C1AB0F16D627DFECEAFD9D7A9B80631E0C33AFA7D26F2F8AA76AE468AC1 5907F3F5F1D9BF030F49C9C00DC86E10246049EBC485E1BA2B44B2A98760D70E

The XML encoded structure of the *StatusReport* message is:

```
<?xml version="1.0" encoding="UTF-8"?>
<Document xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="urn:iso:std:iso:20022:tech:xsd:catm.001.001.06">
 <StsRpt>
    <Hdr>
       <DwnldTrf>false</DwnldTrf>
       <FrmtVrsn>6.0</FrmtVrsn>
       <XchgId>002</XchgId>
       <CreDtTm>2013-12-06T13:53:53.00+02:00</CreDtTm>
       <InitgPty>
          <Id>66000001</Id>
          <Tp>OPOI</Tp>
          <Issr>MTMG</Issr>
       </InitgPty>
       <RcptPty>
          <Id>epas-keyDownload-TM1</Id>
          <Tp>MTMG</Tp>
       </RcptPty>
    </Hdr>
    <StsRpt>
       <POIId>
          <Id>66000001</Id>
          <Tp>OPOI</Tp>
          <Issr>MTMG</Issr>
       </POIId>
       <TermnlMgrId>
          <Id>epas-keyDownload-TM1</Id>
          <Tp>MTMG</Tp>
       </TermnlMgrId>
       <DataSet>
          <Id>
             <Tp>STRP</Tp>
             <CreDtTm>2013-12-06T13:53:53.00+02:00</CreDtTm>
          </Id>
          <Cntt>
             <POICmpnt>
                <Tp>TERM</Tp>
                <Id>
                   <ItmNb>1</ItmNb>
                   <PrvdrId>EPASVendor001</PrvdrId>
                   <Id>Counter Top E41</Id>
                   <SrlNb>7825410759</SrlNb>
                </Id>
             </POICmpnt>
             <POICmpnt>
                <Tp>APLI</Tp>
                <Id>
                   <ItmNb>1.1</ItmNb>
                   <PrvdrId>EPASVendor001</PrvdrId>
                </Id>
                <Sts>
                   <VrsnNb>1.01</VrsnNb>
                </Sts>
                <StdCmplc>
                   <Id>SEPA-FAST</Id>
                   <Vrsn>3.0</Vrsn>
```

```
                <Issr>CIR</Issr>
              </StdCmplc>
            </POICmpnt>
            <AttndncCntxt>ATTD</AttndncCntxt>
            <POIDtTm>2013-12-06T13:53:53.00+02:00</POIDtTm>
            <DataSetReqrd>
              <Id>
                <Nm>epas-acquirer-TM1-TIK</Nm>
                <Tp>SCPR</Tp>
                <Vrsn>20131206135352</Vrsn>
                <CreDtTm>2013-12-06T13:53:52.00+02:00</CreDtTm>
              </Id>
              <POIChllng>
                0Td8cwfWDTm2xvO5M9AImVXWTfTGe2O/YI8/KEHHcFE=
              </POIChllng>
              <TMChllng>
                47DEQpj8HBSa+/TImW+5JCeuQeRkm5NMpJWZG3hSuFU=
              </TMChllng>
              <SsnKey>
                <Id>Key Encryption Key KEK</Id>
                <Vrsn>01</Vrsn>
                <Tp>EDE3</Tp>
                <Fctn>KEYX</Fctn>
                <KeyVal>
                 <CnttTp>EVLP</CnttTp>
                 <EnvlpdData>
                  <Rcpt>
                   <KeyTrnsprt>
                    <Vrsn>0</Vrsn>
                    <RcptId>
                     <IssrAndSrlNb>
                      <Issr>
                       <RltvDstngshdNm>
                        <AttrTp>CATT</AttrTp>
                        <AttrVal>BE</AttrVal>
                       </RltvDstngshdNm>
                       <RltvDstngshdNm>
                        <AttrTp>OATT</AttrTp>
                        <AttrVal>EPASOrg</AttrVal>
                       </RltvDstngshdNm>
                       <RltvDstngshdNm>
                        <AttrTp>OUAT</AttrTp>
                        <AttrVal>Technical Center of Expertise</AttrVal>
                       </RltvDstngshdNm>
                       <RltvDstngshdNm>
                        <AttrTp>CNAT</AttrTp>
                        <AttrVal>EPAS Protocols Test CA</AttrVal>
                       </RltvDstngshdNm>
                      </Issr>
                      <SrlNb>eJXKNQFMPS8eEbEN</SrlNb>
                     </IssrAndSrlNb>
                    </RcptId>
                    <KeyNcrptnAlgo>
                     <Algo>RSAO</Algo>
                      <Param>
                       <DgstAlgo>HS25</DgstAlgo>
                       <MskGnrtrAlgo>
                        <Algo>MGF1</Algo>
                        <Param>
                         <DgstAlgo>HS25</DgstAlgo>
                        </Param>
                       </MskGnrtrAlgo>
                      </Param>
                    </KeyNcrptnAlgo>
                    <NcrptdKey>
                      Do5HCfqDoyuAY1vX0Pf4ue6oFOnSt3o0lYT1JNvfYHZLFs5CcV8B10n8tO+yUXcR
                      pJ39bW+OgYdRnI+nt/+SjsF4PtcH28fVebwImm6qh2zdBhbpMiwKz0MYtCtYNd1b
                      LC/65UYmTWFfeYjg1NxT9iBL1jWxtyTwUfhGk57RE7GjkO5rAuEUErvSTV9zZTIF
                      nVTkjJpnOcHOXUiwppBn6nYkz6RL2L1+/S0+vlh2OYnHSspbOPON0Mju/+5/7Kil
```

```
                        R14OPTKYAHrG6UQqbdMbfTwbrvWm3rM3qv+kg26NCR7vmCrswLpfsF5Ia1HaggJk
                        ICYajwVcQLTzYI17B//CDHFpSp7cKlSLcsrC3Dgtsa/34PYf+QaGAcqQOh8sWY//
                        2IbsI6kl9vNOSb6sQ4Ntdu/Is4j08svmRa0QFMMp6Akso3F8iE2oan+ljo2W2zFX
                        hRpWmPVdugxNJiGg4ViuBoeGlTGvHGsf5MqZscXSHhFpI7kJQn1blJa1gsYtFbpp
                      </NcrptdKey>
                    </KeyTrnsprt>
                  </Rcpt>
                  <NcrptdCntt>
                    <CnttTp>DATA</CnttTp>
                    <CnttNcrptnAlgo>
                      <Algo>E3DC</Algo>
                        <Param>
                          <InitlstnVctr>onu0bRwwbgk=</InitlstnVctr>
                        </Param>
                    </CnttNcrptnAlgo>
                    <NcrptdData>nwQVAnth9GyFHaU1lolOJa0gqPHua6E4</NcrptdData>
                  </NcrptdCntt>
                </EnvlpdData>
              </KeyVal>

            </SsnKey>
          </DataSetReqrd>
        </Cntt>
      </DataSet>
    </StsRpt>
    <SctyTrlr>
      <CnttTp>SIGN</CnttTp>
      <SgndData>
        <DgstAlgo>
          <Algo>HS25</Algo>
        </DgstAlgo>
        <NcpsltdCntt>
          <CnttTp>DATA</CnttTp>
        </NcpsltdCntt>
        <Cert>
          MIIEgzCCAmugAwIBAgIMIiWo+wAHEpPUZBw8MA0GCSqGSIb3DQEBCwUAMGgxCzAJBgNVBAYMAkJFMR
          AwDgYDVQQKDAdFUEFTT3JnMSYwJAYDVQQLDB1UZWNobmljYWwgQ2VudGVyIG9mIEV4cGVydGlzZTEf
          MB0GA1UEAwwWRVBBUyBQcm90b2NvbHMgVGVzdCBDQTAqGBMyMDEzMDQxODEwMjU0NiswMTAwGBMyMD
          E4MTAwMTE4MjAwNSswMTAwMHoxCzAJBgNVBAYMAkZSMRAwDgYDVQQKDAdFUEFTT3JnMSYwJAYDVQQL
          DB1UZWNobmljYWwgQ2VudGVyIG9mIEV4cGVydGlzZTExMC8GA1UEAwwoRVBBUyBQcm90b2NvbCBUZX
          N0IENsaWVudCBBdXRoZW50aWNhdGlvbjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMIl
          ETkLhds5kKJ2OLhQYWwYsRvfeElLSLYfj40DIiWo+wAHEpPUZBw83eGNRzN+tzgawSl2gg/1wLMh5O
          34jJuPFicOD8b6tHBEm6cLlHE5VRq+MmaG9TjE9/Y6Rf9MueZkcACyi3keEgWttqzcKYVGmNkKzDts
          hPD4wu++5OP5hEvXmrFMHyI3YZjBO+rFYN3INRBBdnKcfmL79Ow1DeTThcSNPqQKkNeqWDj67T48dg
          0Zu4TRmXB3xyMx863wULQdtf/RnRKeiMdTMdoTJkvkwvCwoKoJ937tLIAfrSOej+XYtD8QcI/D1gVL
          kVbFtVGE8aKU2rj4JnFivpu1SGcCAwEAAaMPMA0wCwYDVR0PBAQDAgeAMA0GCSqGSIb3DQEBCwUAA4
          ICAQBUDbTMynjFty7DTWpV7nwVLtVECUGeC3vHg7hVlVfALMpegbbMqFSjYlCtygzVXJb0LwGXmbWh
          AMly0/JBHLJnYwDxsJ5Grk8pOiTLce6lRny5GTNxPlVv/MC1WNo0T/T4qzCi+AO9l7tWgQC6xrb66I
          T4Mb+FXE7oI/47rDui2LYV9iwcFoW5vFnfy+HPvf2ynzdz/UZoVoi/ZWZw9buc5WsCnjbnKRYp3mn6
          hYNnYZ2N5PufCGCFGIWkKJStyX3LUdTOv59SCD3VETcbFX49Fvk0ae7Qt/8BvBN9UGXiZqjqPIKZnv
          NiY6hj7V/iKmnkh0/fQaGfpFexLPalKwj3O9O9nC/RM1Ls7k7vYyOCa/ckQPwUnr1YkajW0OXaUFR3
          CFJcpAIbUQWbUrUOYbF2wfliqnrCgJk0Md1b89bBRq26dis+Zynxf6Y52Y1cv9yuVWovwLI3VOSR+X
          vxehjYQqh/jeT7pYtWUXITvFnFEtTwRH8MGXs4eFpFfgoOfdRIBsS6FvgRt6JQJHke10LnQ5LJ1Lq6
          dU8Jth3Y7Cq79nN+SSu8NxhQcqyevqPe8vvVboNriNCAn5aksqyhpbWdGY+UmQuk0qG1DPZMXoOR1t
          yttYyeB05gjX0BIwmpL/3O/ZbNrqT2vl5XKiAWHD1v2Dj/rpZrssZx58g2+zacKA==
        </Cert>
        <Sgnr>
          <SgnrId>
            <IssrAndSrlNb>
              <Issr>
                <RltvDstngshdNm>
                      <AttrTp>CATT</AttrTp>
                      <AttrVal>BE</AttrVal>
                </RltvDstngshdNm>
                <RltvDstngshdNm>
                      <AttrTp>OATT</AttrTp>
                      <AttrVal>EPASOrg</AttrVal>
                </RltvDstngshdNm>
                <RltvDstngshdNm>
```

```
                        <AttrTp>OUAT</AttrTp>
                        <AttrVal>Technical Center of Expertise</AttrVal>
                  </RltvDstngshdNm>
                  <RltvDstngshdNm>
                        <AttrTp>CNAT</AttrTp>
                        <AttrVal>EPAS Protocols Test CA</AttrVal>
                  </RltvDstngshdNm>
               </Issr>
               <SrlNb>IiWo+wAHEpPUZBw8</SrlNb>
            </IssrAndSrlNb>
         </SgnrId>
            <DgstAlgo>
               <Algo>HS25</Algo>
            </DgstAlgo>
            <SgntrAlgo>
               <Algo>ERS2</Algo>
            </SgntrAlgo>
            <Sgntr>
               Ul6RPNJibW31y2eFoyQB0as8WlfDtx8Qc6ehWsQS/41MU0s/5Hy1agybxy+iInnQH3R2tUDFu
               r9IrjkRTltnS9Jr9UY2V/4WW+RT0rv1MfPyVrcJso7fYx2trVdZP9RnGHh5MC3LnjX8p0z8XO
               krbhIq6T2legsnkdRd8wBq33IYN7ury+iR/Z65vRH69B8bbzHJeWe1S3bykEJg+uRRsLxZbWD
               Qr8eCrAuJGdUrJKbXHPEf6ggjgf3rv+yu5X/LSxd8GrDxbWJ9/s6v2depuAYx4MM6+n0m8viq
               dq5GisFZB/P18dm/Aw9JycANyG4QJGBJ68SF4borRLKph2DXDg==
            </Sgntr>
      </Sgnr>
   </SgndData>
 </SctyTrlr>
</StsRpt>
</Document>
```

1.4.6 Configuration Update to Inject Keys

For the following elements, we assume that the TM will use the KEK key sent by the POI to generate through the UKPT algorithm a Session Key. Then this Session key will be used to encipher through a triple DES CBC algorithm the DUKPT initial key to be activated in the POI.

So the security parameters of the TM contain the DUKPT initial key to be activated in the POI:

```
EE3AE644 1C2EEE18 3F3B4179 2DBCD318
```

First, the TM will use the triple DES 112 bits KEK key sent in the previous StatusReport requesting the security parameters data set:

```
A75D20F7 04517545 3E29259D 3B08A72A
```

This TM Host uses the triple DES UKPT transport key mechanism, generating the random string:

```
F5DBFB9D 229BEF77 758F0448 87D15245
```

The triple DES decryption of the two 64 bits blocks of this random string by the KEK key is:

```
A93CBC7A D2303E31 24133B53 A3072276
```

Applying the odd parity to this session key provides the following UKPT key:

```
A83DBC7A D3313E31 25133B52 A2072376
```

The triple DES CBC encryption of the DUKPT initial key by this UKPT key is:

```
8F611CC 30B12BF75 3EA31B1B 7BBC3DDE
```

The header and the body of the *AcceptorConfigurationUpdate* message is presented in the table below:

Message Item	*Value*
Header	
DownloadTransfer	True
FormatVersion	6.0
ExchangeIdentification	002
CreationDateTime	2013-12-06:13:53:54.00+02:00
InitiatingParty	
Identification	66000001
Type	OriginatingPOI
Issuer	MasterTerminalManager
RecipientParty	
Identification	epas-keyDownload-TM1
Type	MasterTerminalManager
AcceptorConfiguration	
TerminalManagerdentification	
Identification	epas-keyDownload-TM1
Type	MasterTerminalManager
DataSet	
Identification	
Type	SecurityParameters
Version	20131206135352
CreationDateTime	2013-12-06:13:53:52.00+02:00
Content	
HostCommunicationParameters	
ActionType	Create

HostIdentification	AcquirerHost1
Key	
KeyIdentification	SpecV1TestKey
KeyVersion	2010060715
SecurityParameters	
ActionType	Create
Version	1.1.01
POIChallenge	D1377C7307D60D39B6C6F3B933D0089955D64DF4C67B63BF608F3F2841C77051
TMChallenge	46FB7DD6C590E232ED8B7B41431D6970362F0D4DBCBD9B24E74C3B3339B312D3
SymetricKey	
Identification	SpecV1TestKey
AdditionalIdentification	398725A501E29020
Version	2010060715
Type	DUKP9
Function	DataEncryption
Function	DataDecryption
Function	PINEncryption
ActivationDate	2013-12-06:13:00:00
KeyValue	
ContentType	EnvelopedData
EnvelopedData	
Recipient	
KEK	
KEKIdentification	
KeyIdentification	KeyEncryptionKey
KeyVersion	2013120613
KeyEncryption-Algorithm	
Algorithm	UKPT
EncryptedKey	F5DBFB9D229BEF77758F044887D15245
EncryptedContent	
ContentType	PlainData
ContentEncryption-Algorithm	
Algorithm	DES112CBC
EncryptedData	8F611CC30B12BF753EA31B1B7BBC3DDE

As for the previous message, the POI has no symmetric key shared usable by the key injection, so the TM authentication RSA key is used to provide a digital signature of the message body.

Once unnecessary spaces and carriage returns are removed, the XML encoded *AcceptorConfigurationUpdate* message body is:

```
0000  3C 41 63 63 70 74 72 43 66 67 74 6E 3E 3C 54 65  |<AccptrCfgtn><Te|
0010  72 6D 6E 6C 4D 67 72 49 64 3E 3C 49 64 3E 65 70  |rmnlMgrId><Id>ep|
0020  61 73 2D 6B 65 79 44 6F 77 6E 6C 6F 61 64 2D 54  |as-keyDownload-T|
0030  4D 31 3C 2F 49 64 3E 3C 54 70 3E 4D 54 4D 47 3C  |M1</Id><Tp>MTMG<|
0040  2F 54 70 3E 3C 2F 54 65 72 6D 6E 6C 4D 67 72 49  |/Tp></TermnlMgrI|
0050  64 3E 3C 44 61 74 61 53 65 74 3E 3C 49 64 3E 3C  |d><DataSet><Id><|
0060  54 70 3E 53 43 50 52 3C 2F 54 70 3E 3C 56 72 73  |Tp>SCPR</Tp><Vrs|
0070  6E 3E 32 30 31 33 31 32 30 36 31 33 35 33 35 32  |n>20131206135352|
0080  3C 2F 56 72 73 6E 3E 3C 43 72 65 44 74 54 6D 3E  |</Vrsn><CreDtTm>|
0090  32 30 31 33 2D 31 32 2D 30 36 54 31 33 3A 35 33  |2013-12-06T13:53|
00A0  3A 35 32 2E 30 30 2B 30 32 3A 30 30 3C 2F 43 72  |:52.00+02:00</Cr|
00B0  65 44 74 54 6D 3E 3C 2F 49 64 3E 3C 43 6E 74 74  |eDtTm></Id><Cntt|
00C0  3E 3C 48 73 74 43 6F 6D 50 61 72 61 6D 73 3E 3C  |><HstComParams><|
00D0  41 63 74 6E 54 70 3E 43 52 45 41 3C 2F 41 63 74  |ActnTp>CREA</Act|
00E0  6E 54 70 3E 3C 48 73 74 49 64 3E 41 63 71 75 69  |nTp><HstId>Acqui|
00F0  72 65 72 48 6F 73 74 31 3C 2F 48 73 74 49 64 3E  |rerHost1</HstId>|
0100  3C 4B 65 79 3E 3C 4B 65 79 49 64 3E 53 70 65 63  |<Key><KeyId>Spec|
0110  56 31 54 65 73 74 4B 65 79 3C 2F 4B 65 79 49 64  |V1TestKey</KeyId|
0120  3E 3C 4B 65 79 56 72 73 6E 3E 32 30 31 30 30 36  |><KeyVrsn>201006|
0130  30 37 31 35 3C 2F 4B 65 79 56 72 73 6E 3E 3C 2F  |0715</KeyVrsn></|
0140  4B 65 79 3E 3C 2F 48 73 74 43 6F 6D 50 61 72 61  |Key></HstComPara|
0150  6D 73 3E 3C 53 63 74 79 50 61 72 61 6D 73 3E 3C  |ms><SctyParams><|
0160  41 63 74 6E 54 70 3E 43 52 45 41 3C 2F 41 63 74  |ActnTp>CREA</Act|
0170  6E 54 70 3E 3C 56 72 73 6E 3E 31 2E 31 2E 30 31  |nTp><Vrsn>1.1.01|
0180  3C 2F 56 72 73 6E 3E 3C 50 4F 49 43 68 6C 6C 6E  |</Vrsn><POIChlln|
0190  67 3E 30 54 64 38 63 77 66 57 44 54 6D 32 78 76  |g>0Td8cwfWDTm2xv|
01A0  4F 35 4D 39 41 49 6D 56 58 57 54 66 54 47 65 32  |O5M9AImVXWTfTGe2|
01B0  4F 2F 59 49 38 2F 4B 45 48 48 63 46 45 3D 3C 2F  |O/YI8/KEHHcFE=</|
01C0  50 4F 49 43 68 6C 6C 6E 67 3E 3C 54 4D 43 68 6C  |POIChllng><TMChl|
01D0  6C 6E 67 3E 52 76 74 39 31 73 57 51 34 6A 4C 74  |lng>Rvt91sWQ4jLt|
01E0  69 33 74 42 51 78 31 70 63 44 59 76 44 55 32 38  |i3tBQx1pcDYvDU28|
01F0  76 5A 73 6B 35 30 77 37 4D 7A 6D 7A 45 74 4D 3D  |vZsk50w7MzmzEtM=|
0200  3C 2F 54 4D 43 68 6C 6C 6E 67 3E 3C 53 6D 6D 74  |</TMChllng><Smmt|
0210  72 63 4B 65 79 3E 3C 49 64 3E 53 70 65 63 56 31  |rcKey><Id>SpecV1|
0220  54 65 73 74 4B 65 79 3C 2F 49 64 3E 3C 41 64 64  |TestKey</Id><Add|
0230  74 6C 49 64 3E 4F 59 63 6C 70 51 48 69 6B 43 41  |tlId>OYclpQHikCA|
0240  3D 3C 2F 41 64 64 74 6C 49 64 3E 3C 56 72 73 6E  |=</AddtlId><Vrsn|
0250  3E 32 30 31 30 30 36 30 37 31 35 3C 2F 56 72 73  |>2010060715</Vrs|
0260  6E 3E 3C 54 70 3E 44 4B 50 39 3C 2F 54 70 3E 3C  |n><Tp>DKP9</Tp><|
0270  46 63 74 6E 3E 44 45 4E 43 3C 2F 46 63 74 6E 3E  |Fctn>DENC</Fctn>|
0280  3C 46 63 74 6E 3E 44 44 45 43 3C 2F 46 63 74 6E  |<Fctn>DDEC</Fctn|
0290  3E 3C 46 63 74 6E 3E 50 49 4E 45 3C 2F 46 63 74  |><Fctn>PINE</Fct|
02A0  6E 3E 3C 41 63 74 76 74 6E 44 74 3E 32 30 31 33  |n><ActvtnDt>2013|
02B0  2D 31 32 2D 30 36 54 31 33 3A 30 30 3A 30 30 3C  |-12-06T13:00:00<|
02C0  2F 41 63 74 76 74 6E 44 74 3E 3C 4B 65 79 56 61  |/ActvtnDt><KeyVa|
02D0  6C 3E 3C 43 6E 74 74 54 70 3E 45 56 4C 50 3C 2F  |l><CnttTp>EVLP</|
02E0  43 6E 74 74 54 70 3E 3C 45 6E 76 6C 70 64 44 61  |CnttTp><EnvlpdDa|
02F0  74 61 3E 3C 52 63 70 74 3E 3C 4B 45 4B 3E 3C 4B  |ta><Rcpt><KEK><K|
0300  45 4B 49 64 3E 3C 4B 65 79 49 64 3E 4B 65 79 45  |EKId><KeyId>KeyE|
```

```
0310  6E 63 72 79 70 74 69 6F 6E 4B 65 79 3C 2F 4B 65  |ncryptionKey</Ke|
0320  79 49 64 3E 3C 4B 65 79 56 72 73 6E 3E 32 30 31  |yId><KeyVrsn>201|
0330  33 31 32 30 36 31 33 3C 2F 4B 65 79 56 72 73 6E  |3120613</KeyVrsn|
0340  3E 3C 2F 4B 45 4B 49 64 3E 3C 4B 65 79 4E 63 72  |></KEKId><KeyNcr|
0350  70 74 6E 41 6C 67 6F 3E 3C 41 6C 67 6F 3E 55 4B  |ptnAlgo><Algo>UK|
0360  50 54 3C 2F 41 6C 67 6F 3E 3C 2F 4B 65 79 4E 63  |PT</Algo></KeyNc|
0370  72 70 74 6E 41 6C 67 6F 3E 3C 4E 63 72 70 74 64  |rptnAlgo><Ncrptd|
0380  4B 65 79 3E 39 64 76 37 6E 53 4B 62 37 33 64 31  |Key>9dv7nSKb73d1|
0390  6A 77 52 49 68 39 46 53 52 51 3D 3D 3C 2F 4E 63  |jwRIh9FSRQ==</Nc|
03A0  72 70 74 64 4B 65 79 3E 3C 2F 4B 45 4B 3E 3C 2F  |rptdKey></KEK></|
03B0  52 63 70 74 3E 3C 4E 63 72 70 74 64 43 6E 74 74  |Rcpt><NcrptdCntt|
03C0  3E 3C 43 6E 74 74 54 70 3E 44 41 54 41 3C 2F 43  |><CnttTp>DATA</C|
03D0  6E 74 74 54 70 3E 3C 43 6E 74 74 4E 63 72 70 74  |nttTp><CnttNcrpt|
03E0  6E 41 6C 67 6F 3E 3C 41 6C 67 6F 3E 45 33 44 43  |nAlgo><Algo>E3DC|
03F0  3C 2F 41 6C 67 6F 3E 3C 2F 43 6E 74 74 4E 63 72  |</Algo></CnttNcr|
0400  70 74 6E 41 6C 67 6F 3E 3C 4E 63 72 70 74 64 44  |ptnAlgo><NcrptdD|
0410  61 74 61 3E 6A 32 45 63 77 77 73 53 76 33 55 2B  |ata>j2EcwwsSv3U+|
0420  6F 78 73 62 65 37 77 39 33 67 3D 3D 3C 2F 4E 63  |oxsbe7w93g==</Nc|
0430  72 70 74 64 44 61 74 61 3E 3C 2F 4E 63 72 70 74  |rptdData></Ncrpt|
0440  64 43 6E 74 74 3E 3C 2F 45 6E 76 6C 70 64 44 61  |dCntt></EnvlpdDa|
0450  74 61 3E 3C 2F 4B 65 79 56 61 6C 3E 3C 2F 53 6D  |ta></KeyVal></Sm|
0460  6D 74 72 63 4B 65 79 3E 3C 2F 53 63 74 79 50 61  |mtrcKey></SctyPa|
0470  72 61 6D 73 3E 3C 2F 43 6E 74 74 3E 3C 2F 44 61  |rams></Cntt></Da|
0480  74 61 53 65 74 3E 3C 2F 41 63 63 70 74 72 43 66  |taSet></AccptrCf|
0490  67 74 6E 3E                                      |gtn>            |
```

The SHA256 digest of the *AcceptorConfigurationUpdate* message body is:

```
0000  02 2D 5E 14 AE DF 94 96 11 1C FE F2 44 90 A0 A8  |.-^.........D...|
0010  9F 55 9B DA 21 0E 56 13 FC 84 1A 05 96 09 96 3F  |.U..!.V........?|
```

Applying the padding process for the digital signature, the block result is dumped below:

```
0000  00 01 FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0010  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0020  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0030  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0040  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0050  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0060  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0070  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0080  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0090  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
00A0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
00B0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
00C0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
00D0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
00E0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
00F0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0100  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0110  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0120  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0130  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0140  FF FF FF FF FF FF FF FF FF FF FF FF 00 30 31 30  |.............010|
0150  0D 06 09 60 86 48 01 65 03 04 02 01 05 00 04 20  |...`.H.e....... |
```

```
0160  02 2D 5E 14 AE DF 94 96 11 1C FE F2 44 90 A0 A8  |.-^.........D...|
0170  9F 55 9B DA 21 0E 56 13 FC 84 1A 05 96 09 96 3F  |.U..!.V........?|
```

After encryption by the private key of $K_{TM\text{-}Sign}$, we have the digital signature of the *AcceptorConfigurationUpdate* message body:

```
0000  09 55 30 7F 9E 97 53 57 67 C5 DC 9F CE 1D 85 C7  |.U0...SWg.......|
0010  46 EE 4B BD 6E 10 4A 55 0E 23 C7 AF 1F 7C 9E 24  |F.K.n.JU.#...|.$|
0020  31 DA 8D 7E 67 E4 3B A8 03 0F 5B DB 92 8F 47 6B  |1..~g.;...[...Gk|
0030  CB 65 16 30 95 0F E6 98 B7 0D 8F 69 77 38 2A 19  |.e.0.......iw8*.|
0040  91 88 A5 63 D9 07 A9 F5 88 E8 65 6A 61 27 C7 27  |...c......eja'.'|
0050  A6 CA 3B 2C FB A4 84 C9 91 5E BD FB 4D 99 57 48  |..;,.....^..M.WH|
0060  DC 19 F9 D9 70 7F 50 B2 CF 5F 8B A0 47 9F 99 11  |....p.P.._..G...|
0070  35 EB F4 A8 26 ED EB 52 50 85 DC 70 72 12 5D D2  |5...&..RP..pr.].|
0080  3F 09 FF 6A B7 7F A7 8E 4A FC 35 5F 60 E9 23 3C  |?..j....J.5_`.#<|
0090  F2 40 FD F5 13 43 EF 0C E9 46 0B 7F B7 99 98 7B  |.@...C...F.....{|
00A0  6E E4 F4 F7 EE 41 C2 83 EF 40 A7 14 DB 9F AC 61  |n....A...@.....a|
00B0  ED FF 64 59 BD 44 6F 58 8C 23 35 6F B9 6A FE 0C  |..dY.DoX.#5o.j..|
00C0  BD B5 B9 B2 4C 64 CF 65 71 1B 07 D1 F1 45 7F AE  |....Ld.eq....E..|
00D0  B1 BB F3 9D 8E E9 40 CD 71 D0 66 AE 7F 86 4D 11  |......@.q.f...M.|
00E0  E1 73 95 80 77 E4 A0 8B 93 87 03 1F 86 8E F2 22  |.s..w..........."|
00F0  EC 70 88 7C 37 29 24 EC 34 3A 87 FB B0 30 83 A7  |.p.|7)$.4:...0..|
0100  6B 69 07 FD BA 54 C1 26 19 AA F7 6C 22 C3 48 D4  |ki...T.&...l".H.|
0110  C0 BA 3F 90 2F FE 13 BB 63 4C EC 4B 58 73 A0 E0  |..?./...cL.KXs..|
0120  09 F2 1D CD C4 87 C7 2B 6A 19 3C F9 67 2F CA 56  |.......+j.<.g/.V|
0130  DD 1D 2C AA 25 8D 06 DF FB DE 9E 33 F2 75 E9 AA  |..,.%......3.u..|
0140  9C F9 94 68 EA 56 C8 E9 A2 25 3E 5A 34 13 AF 01  |...h.V...%>Z4...|
0150  29 99 0B 96 72 1F 76 12 2D 32 88 F4 72 E0 08 D4  |)...r.v.-2..r...|
0160  D3 21 44 32 31 0E 9C AC 6B 66 EF 94 B3 85 97 9C  |.!D21...kf......|
0170  3C E1 2E 75 CD AD 58 E9 28 53 46 AB 0A A7 F1 ED  |<..u..X.(SF.....|
```

2090 Inside the *SecurityTrailer*, the *SignedData* CMS data structure is presented in the table below:

Message Item	*Value*
SecurityTrailer	
SignedData	
ContentType	SignedData
DigestAlgorithm	
Algorithm	SHA256
EncapsulatedContent	
ContentType	PlainData
Certificate	308204FF308202E7A003020102020A2ABC40F4D482F5EBC975300D06092A8648 86F70D01010B05003068310B300906035504060C0242453110300E060355040A 0C07455041534F726731263024060355040B0C1D546563686E6963616C204365 6E746572206F66204578706572746973653 11F301D06035504030C1645504153 2050726F746F636F6C732054657374204341302A181332303133303431383130 303634362B303130301813323031383130303131383230303052B303130303078 310B300906035504060C0246523110300E060355040A0C07455041534F726731 263024060355040B0C1D546563686E6963616C2043656E746572206F66204578 706572746973653 12F302D06035504030C26455041532050726F746F636F6C20 5465737420486F737420417574686E7469636174696F6E308201A2300D0609 2A864886F70D01010105000382018F003082018A0282018100BD095898F981BA F42BE20E19339B396C59626690BDF396D20C503CA57C688AF41E50552CF1B9DD C4116209DD00C26B673F7EDEE7D0CA6DC2DAA9FF2F8C3A860B8F835AE60D9E05 7EDDF1625FAC55A102837FC1C7EF8C0A6C137C5973972ABC40F4D482F5EBC975 4F964B6EECEDBE66DB62AD0DA7B38E05917562E899DF717D27457693B41E7BF2 CBA98855AE2C97DE4B48FD812A520D6D356010F6E8355EC98DBA3047F2C0CDCD 9BE655277F3ED69A788DD80A6A12BCA3D4C7F08662B99D3F70A9548D7804B5E4 A2913A3EC02525BE639ED7D9B986556C5932675642FCC4E659D828A94C5544AE BBC5446EE6B96A04A0185470296DFC2FFBA73D4074930968DD810E43D574DD7B E664899DA6E48EB4B3B590E2CAA97C75015C735093AD62E3FD791AB5718F1FA1
Signer	
SignerIdentification	
IssuerAnd-SerialNumber	
Issuer	
RelativeDistin-guishedName	
AttributeType	CountryName
AttributeValue	BE
RelativeDistin-guishedName	
AttributeType	OrganisationName
AttributeValue	EPASOrg
RelativeDistin-guishedName	
AttributeType	OrganisationUnitName
AttributeValue	Technical Center of Expertise
RelativeDistin-guishedName	
AttributeType	CommonName
AttributeValue	EPAS Protocols Test CA
SerialNumber	2ABC40F4D482F5EBC975
DigestAlgorithm	
Algorithm	SHA256
SignatureAlgorithm	
Algorithm	SHA256WithRSA

Signature	0955307F9E97535767C5DC9FCE1D85C746EE4BBD6E104A550E23C7AF1F7C9E24 31DA8D7E67E43BA8030F5BDB928F476BCB651630950FE698B70D8F6977382A19 9188A563D907A9F588E8656A6127C727A6CA3B2CFBA484C9915EBDFB4D995748 DC19F9D9707F50B2CF5F8BA0479F991135EBF4A826EDEB525085DC7072125DD2 3F09FF6AB77FA78E4AFC355F60E9233CF240FDF51343EF0CE9460B7FB799987B 6EE4F4F7EE41C283EF40A714DB9FAC61EDFF6459BD446F588C23356FB96AFE0C BDB5B9B24C64CF65711B07D1F1457FAEB1BBF39D8EE940CD71D066AE7F864D11 E173958077E4A08B9387031F868EF222EC70887C372924EC343A87FBB03083A7 6B6907FDBA54C12619AAF76C22C348D4C0BA3F902FFE13BB634CEC4B5873A0E0 09F21DCDC487C72B6A193CF9672FCA56DD1D2CAA258D06DFFBDE9E33F275E9AA 9CF99468EA56C8E9A2253E5A3413AF0129990B96721F76122D3288F472E008D4 D3214432310E9CAC6B66EF94B385979C3CE12E75CDAD58E9285346AB0AA7F1ED

The XML encoded structure of the *AcceptorConfigurationUpdate* message is:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<Document xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="urn:iso:std:iso:20022:tech:xsd:catm.003.001.06">
 <AccptrCfgtnUpd>
    <Hdr>
       <DwnldTrf>true</DwnldTrf>
       <FrmtVrsn>6.0</FrmtVrsn>
       <XchgId>002</XchgId>
       <CreDtTm>2013-12-06T13:53:54.00+02:00</CreDtTm>
       <InitgPty>
          <Id>66000001</Id>
          <Tp>OPOI</Tp>
          <Issr>MTMG</Issr>
       </InitgPty>
       <RcptPty>
          <Id>epas-keyDownload-TM1</Id>
          <Tp>MTMG</Tp>
       </RcptPty>
    </Hdr>
    <AccptrCfgtn>
       <TermnlMgrId>
          <Id>epas-keyDownload-TM1</Id>
          <Tp>MTMG</Tp>
       </TermnlMgrId>
       <DataSet>
          <Id>
             <Tp>SCPR</Tp>
             <Vrsn>20131206135352</Vrsn>
             <CreDtTm>2013-12-06T13:53:52.00+02:00</CreDtTm>
          </Id>
          <Cntt>
             <HstComParams>
                <ActnTp>CREA</ActnTp>
                <HstId>AcquirerHost1</HstId>
                <Key>
                   <KeyId>SpecV1TestKey</KeyId>
                   <KeyVrsn>2010060715</KeyVrsn>
              </Key>
             </HstComParams>
             <SctyParams>
                <ActnTp>CREA</ActnTp>
                <Vrsn>1.1.01</Vrsn>
                <POIChllng>0Td8cwfWDTm2xvO5M9AImVXWTfTGe2O/YI8/KEHHcFE=</POIChllng>
                <TMChllng>Rvt91sWQ4jLti3tBQx1pcDYvDU28vZsk50w7MzmzEtM=</TMChllng>
                <SmmtrcKey>
                   <Id>SpecV1TestKey</Id>
                   <AddtlId>OYclpQHikCA=</AddtlId>
                   <Vrsn>2010060715</Vrsn>
                   <Tp>DKP9</Tp>
                   <Fctn>DENC</Fctn>
                   <Fctn>DDEC</Fctn>
                   <Fctn>PINE</Fctn>
                   <ActvtnDt>2013-12-06T13:00:00</ActvtnDt>
                   <KeyVal>
```

```
                  <CnttTp>EVLP</CnttTp>
                  <EnvlpdData>
                     <Rcpt>
                      <KEK>
                         <KEKId>
                           <KeyId>KeyEncryptionKey</KeyId>
                           <KeyVrsn>2013120613</KeyVrsn>
                         </KEKId>
                         <KeyNcrptnAlgo>
                           <Algo>UKPT</Algo>
                         </KeyNcrptnAlgo>
                         <NcrptdKey>9dv7nSKb73d1jwRIh9FSRQ==</NcrptdKey>
                      </KEK>
                     </Rcpt>
                     <NcrptdCntt>
                      <CnttTp>DATA</CnttTp>
                      <CnttNcrptnAlgo>
                         <Algo>E3DC</Algo>
                      </CnttNcrptnAlgo>
                      <NcrptdData>j2EcwwsSv3U+oxsbe7w93g==</NcrptdData>
                     </NcrptdCntt>
                  </EnvlpdData>
               </KeyVal>
            </SmmtrcKey>
         </SctyParams>
      </Cntt>
   </DataSet>
 </AccptrCfgtn>
<SctyTrlr>
 <CnttTp>SIGN</CnttTp>
 <SgndData>
   <DgstAlgo>
      <Algo>HS25</Algo>
   </DgstAlgo>
   <NcpsltdCntt>
      <CnttTp>DATA</CnttTp>
   </NcpsltdCntt>
   <Cert>
      MIIEgzCCAmugAwIBAgIMIiWo+wAHEpPUZBw8MA0GCSqGSIb3DQEBCwUAMGgxCzAJBgNVBAYMAkJFMR
      AwDgYDVQQKDAdFUEFTT3JnMSYwJAYDVQQLDB1UZWNobmljYWwgQ2VudGVyIG9mIEV4cGVydGlzZTEf
      MB0GA1UEAwwRVBBUyBQcm90b2NvbHMgVGVzdCBDQTAqGBMyMDEzMDQxODEwMjU0NiswMTAwGBMyMD
      E4MTAwMTE4MjAwNSswMTAwMHoxCzAJBgNVBAYMAkZSMRAwDgYDVQQKDAdFUEFTT3JnMSYwJAYDVQQL
      DB1UZWNobmljYWwgQ2VudGVyIG9mIEV4cGVydGlzZTExMC8GA1UEAwoRVBBUyBQcm90b2NvbCBUZX
      N0IENsaWVudCBBdXRoZW50aWNhdGlvbjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMIl
      ETkLhds5kKJ2OLhQYWwYsRvfeElLSLYfj40DIiWo+wAHEpPUZBw83eGNRzN+tzgawSl2gg/1wLMh5O
      34jJuPFicOD8b6tHBEm6cLlHE5VRq+MmaG9TjE9/Y6Rf9MueZkcACyi3keEgWttqzcKYVGmNkKzDts
      hPD4wu++5OP5hEvXmrFMHyI3YZjBO+rFYN3INRBBdnKcfmL79Ow1DeTThcSNPqQKkNeqWDj67T48dg
      0Zu4TRmXB3xyMx863wULQdtf/RnRKeiMdTMdoTJkvkwvCwoKoJ937tLIAfrSOej+XYtD8QcI/D1gVL
      kVbFtVGE8aKU2rj4JnFivpu1SGcCAwEAAaMPMA0wCwYDVR0PBAQDAgeAMA0GCSqGSIb3DQEBCwUAA4
      ICAQBUDbTMynjFty7DTWpV7nwVLtVECUGeC3vHg7hVlVfALMpegbbMqFSjYlCtygzVXJb0LwGXmbWh
      AMly0/JBHLJnYwDxsJ5Grk8pOiTLce6lRny5GTNxPlVv/MC1WNo0T/T4qzCi+AO9l7tWgQC6xrb66I
      T4Mb+FXE7oI/47rDui2LYV9iwcFoW5vFnfy+HPvf2ynzdz/UZoVoi/ZWZw9buc5WsCnjbnKRYp3mn6
      hYNnYZ2N5PufCGCFGIWkKJStyX3LUdTOv59SCD3VETcbFX49Fvk0ae7Qt/8BvBN9UGXiZqjqPIKZnv
      NiY6hj7V/iKmnkh0/fQaGfpFexLPalKwj3O9O9nC/RM1Ls7k7vYyOCa/ckQPwUnr1YkajW0OXaUFR3
      CFJcpAIbUQWbUrUOYbF2wfliqnrCgJk0Md1b89bBRq26dis+Zynxf6Y52Y1cv9yuVWovwLI3VOSR+X
      vxehjYQqh/jeT7pYtWUXITvFnFEtTwRH8MGXs4eFpFfgoOfdRIBsS6FvgRt6JQJHke10LnQ5LJ1Lq6
      dU8Jth3Y7Cq79nN+SSu8NxhQcqyevqPe8vvVboNriNCAn5aksqyhpbWdGY+UmQuk0qG1DPZMXoOR1t
      yttYyeB05gjX0BIwmpL/3O/ZbNrqT2vl5XKiAWHD1v2Dj/rpZrssZx58g2+zacKA==
   </Cert>
   <Sgnr>
      <SgnrId>
         <IssrAndSrlNb>
            <Issr>
               <RltvDstngshdNm>
                <AttrTp>CATT</AttrTp>
                <AttrVal>BE</AttrVal>
               </RltvDstngshdNm>
               <RltvDstngshdNm>
                <AttrTp>OATT</AttrTp>
```

```
                  <AttrVal>EPASOrg</AttrVal>
                </RltvDstngshdNm>
                <RltvDstngshdNm>
                  <AttrTp>OUAT</AttrTp>
                  <AttrVal>Technical Center of Expertise</AttrVal>
                </RltvDstngshdNm>
                <RltvDstngshdNm>
                  <AttrTp>CNAT</AttrTp>
                  <AttrVal>EPAS Protocols Test CA</AttrVal>
                </RltvDstngshdNm>
              </Issr>
              <SrlNb>IiWo+wAHEpPUZBw8</SrlNb>
            </IssrAndSrlNb>
          </SgnrId>
            <DgstAlgo>
              <Algo>HS25</Algo>
            </DgstAlgo>
            <SgntrAlgo>
              <Algo>ERS2</Algo>
            </SgntrAlgo>
            <Sgntr>
              CVUwf56XU1dnxdyfzh2Fx0buS71uEEpVDiPHrx98niQx2o1+Z+Q7qAMPW9uSj0dry2UWMJUP5p
              i3DY9pdzgqGZGIpWPZB6n1iOhlamEnxyemyjss+6SEyZFevftNmVdI3Bn52XB/ULLPX4ugR5+Z
              ETXr9Kgm7etSUIXccHISXdI/Cf9qt3+njkr8NV9g6SM88kD99RND7wzpRgt/t5mYe27k9PfuQc
              KD70CnFNufrGHt/2RZvURvWIwjNW+5av4MvbW5skxkz2VxGwfR8UV/rrG7852O6UDNcdBmrn+G
              TRHhc5WAd+Sgi5OHAx+GjvIi7HCIfDcpJOw0Oof7sDCDp2tpB/26VMEmGar3bCLDSNTAuj+QL/
              4Tu2NM7EtYc6DgCfIdzcSHxytqGTz5Zy/KVt0dLKoljQbf+96eM/J16aqc+ZRo6lbI6aIlPlo0
              E68BKZkLlnIfdhItMoj0cuAI1NMhRDIxDpysa2bvlLOFl5w84S51za1Y6ShTRqsKp/Ht
            </Sgntr>
        </Sgnr>
    </SgndData>
  </SctyTrlr>
</AccptrCfgtnUpd>
</Document>
```

1.4.7 Key Download Result

The POI sends a *StatusReport* message to report the result of the key download action with the new activated key.

The triple DES CBC encryption of 8 null bytes with the key `EE3AE644 1C2EEE18 3F3B4179 2DBCD318` (without extension) is:

```
4E06B7DB F79A7705
```

The *StatusReport* message containing the header and the body presented in the table below:

Message Item	*Value*
Header	
DownloadTransfer	False
FormatVersion	6.0
ExchangeIdentification	003
CreationDateTime	2013-12-06:13:53:55.00+02:00
InitiatingParty	
Identification	66000001
Type	OriginationgPOI
Issuer	MasterTerminalManager
RecipientParty	
Identification	epas-keyDownload-TM1
Type	MasterTerminalManager
StatusReport	
POIIdentification	
Identification	66000001
Type	OriginationgPOI
Issuer	MasterTerminalManager
TerminalManagerdentification	
Identification	epas-keyDownload-TM1
Type	MasterTerminalManager
DataSet	
Identification	
Type	StatusReport
CreationDateTime	2013-12-06:13:53:55.00+02:00
Content	
Component	
Type	Terminal
Identification	
ItemNumber	1
ProviderIdentification	EPASVendor001
Identification	Counter Top E41
SerialNumber	7825410759
Component	
Type	PaymentApplication
Identification	
ItemNumber	1.1
ProviderIdentification	EPASVendor001
Status	

VersionNumber	1.01
StandardCompliance	
Identification	SEPA-FAST
VersionNumber	3.0
Issuer	CIR
Component	
Type	SecurityParameters
Identification	
ItemNumber	1.1
ProviderIdentification	EPASVendor001
Identification	SpecV1TestKey
Status	
VersionNumber	2010060715
Status	InOperation
Characteristics	
KeyCheckValue	4E06B7DBF79A7705
AttendanceContext	Attended
POIDateTime	2013-12-06T13:53:55.00+02:00

Once unnecessary spaces and carriage returns are removed, the XML encoded *StatusReport* message body is:

```
0000  3C 53 74 73 52 70 74 3E 3C 50 4F 49 49 64 3E 3C  |<StsRpt><POIId><|
0010  49 64 3E 36 36 30 30 30 30 30 31 3C 2F 49 64 3E  |Id>66000001</Id>|
0020  3C 54 70 3E 4F 50 4F 49 3C 2F 54 70 3E 3C 49 73  |<Tp>OPOI</Tp><Is|
0030  73 72 3E 4D 54 4D 47 3C 2F 49 73 73 72 3E 3C 2F  |sr>MTMG</Issr></|
0040  50 4F 49 49 64 3E 3C 54 65 72 6D 6E 6C 4D 67 72  |POIId><TermnlMgr|
0050  49 64 3E 3C 49 64 3E 65 70 61 73 2D 6B 65 79 44  |Id><Id>epas-keyD|
0060  6F 77 6E 6C 6F 61 64 2D 54 4D 31 3C 2F 49 64 3E  |ownload-TM1</Id>|
0070  3C 54 70 3E 4D 54 4D 47 3C 2F 54 70 3E 3C 2F 54  |<Tp>MTMG</Tp></T|
0080  65 72 6D 6E 6C 4D 67 72 49 64 3E 3C 44 61 74 61  |ermnlMgrId><Data|
0090  53 65 74 3E 3C 49 64 3E 3C 54 70 3E 53 54 52 50  |Set><Id><Tp>STRP|
00A0  3C 2F 54 70 3E 3C 43 72 65 44 74 54 6D 3E 32 30  |</Tp><CreDtTm>20|
00B0  31 33 2D 31 32 2D 30 36 54 31 33 3A 35 33 3A 35  |13-12-06T13:53:5|
00C0  35 2E 30 30 2B 30 32 3A 30 30 3C 2F 43 72 65 44  |5.00+02:00</CreD|
00D0  74 54 6D 3E 3C 2F 49 64 3E 3C 43 6E 74 74 3E 3C  |tTm></Id><Cntt><|
00E0  50 4F 49 43 6D 70 6E 74 3E 3C 54 70 3E 54 45 52  |POICmpnt><Tp>TER|
00F0  4D 3C 2F 54 70 3E 3C 49 64 3E 3C 49 74 6D 4E 62  |M</Tp><Id><ItmNb|
0100  3E 31 3C 2F 49 74 6D 4E 62 3E 3C 50 72 76 64 72  |>1</ItmNb><Prvdr|
0110  49 64 3E 45 50 41 53 56 65 6E 64 6F 72 30 30 31  |Id>EPASVendor001|
0120  3C 2F 50 72 76 64 72 49 64 3E 3C 49 64 3E 43 6F  |</PrvdrId><Id>Co|
0130  75 6E 74 65 72 20 54 6F 70 20 45 34 31 3C 2F 49  |unter Top E41</I|
0140  64 3E 3C 53 72 6C 4E 62 3E 37 38 32 35 34 31 30  |d><SrlNb>7825410|
0150  37 35 39 3C 2F 53 72 6C 4E 62 3E 3C 2F 49 64 3E  |759</SrlNb></Id>|
0160  3C 2F 50 4F 49 43 6D 70 6E 74 3E 3C 50 4F 49 43  |</POICmpnt><POIC|
0170  6D 70 6E 74 3E 3C 54 70 3E 41 50 4C 49 3C 2F 54  |mpnt><Tp>APLI</T|
0180  70 3E 3C 49 64 3E 3C 49 74 6D 4E 62 3E 31 2E 31  |p><Id><ItmNb>1.1|
0190  3C 2F 49 74 6D 4E 62 3E 3C 50 72 76 64 72 49 64  |</ItmNb><PrvdrId|
01A0  3E 45 50 41 53 56 65 6E 64 6F 72 30 30 31 3C 2F  |>EPASVendor001</|
01B0  50 72 76 64 72 49 64 3E 3C 2F 49 64 3E 3C 53 74  |PrvdrId></Id><St|
01C0  73 3E 3C 56 72 73 6E 4E 62 3E 31 2E 30 31 3C 2F  |s><VrsnNb>1.01</|
01D0  56 72 73 6E 4E 62 3E 3C 2F 53 74 73 3E 3C 53 74  |VrsnNb></Sts><St|
01E0  64 43 6D 70 6C 63 3E 3C 49 64 3E 53 45 50 41 2D  |dCmplc><Id>SEPA-|
```

```
01F0  46 41 53 54 3C 2F 49 64 3E 3C 56 72 73 6E 3E 33  |FAST</Id><Vrsn>3|
0200  2E 30 3C 2F 56 72 73 6E 3E 3C 49 73 73 72 3E 43  |.0</Vrsn><Issr>C|
0210  49 52 3C 2F 49 73 73 72 3E 3C 2F 53 74 64 43 6D  |IR</Issr></StdCm|
0220  70 6C 63 3E 3C 2F 50 4F 49 43 6D 70 6E 74 3E 3C  |plc></POICmpnt><|
0230  50 4F 49 43 6D 70 6E 74 3E 3C 54 70 3E 53 43 50  |POICmpnt><Tp>SCP|
0240  52 3C 2F 54 70 3E 3C 49 64 3E 3C 49 74 6D 4E 62  |R</Tp><Id><ItmNb|
0250  3E 31 2E 31 3C 2F 49 74 6D 4E 62 3E 3C 50 72 76  |>1.1</ItmNb><Prv|
0260  64 72 49 64 3E 45 50 41 53 56 65 6E 64 6F 72 30  |drId>EPASVendor0|
0270  30 31 3C 2F 50 72 76 64 72 49 64 3E 3C 49 64 3E  |01</PrvdrId><Id>|
0280  53 70 65 63 56 31 54 65 73 74 4B 65 79 3C 2F 49  |SpecV1TestKey</I|
0290  64 3E 3C 2F 49 64 3E 3C 53 74 73 3E 3C 56 72 73  |d></Id><Sts><Vrs|
02A0  6E 4E 62 3E 32 30 31 30 30 36 30 37 31 35 3C 2F  |nNb>2010060715</|
02B0  56 72 73 6E 4E 62 3E 3C 53 74 73 3E 4F 50 45 52  |VrsnNb><Sts>OPER|
02C0  3C 2F 53 74 73 3E 3C 2F 53 74 73 3E 3C 43 68 72  |</Sts></Sts><Chr|
02D0  74 63 73 3E 3C 4B 65 79 43 68 63 6B 56 61 6C 3E  |tcs><KeyChckVal>|
02E0  54 67 61 33 32 2F 65 61 64 77 55 3D 3C 2F 4B 65  |Tga32/eadwU=</Ke|
02F0  79 43 68 63 6B 56 61 6C 3E 3C 2F 43 68 72 74 63  |yChckVal></Chrtc|
0300  73 3E 3C 2F 50 4F 49 43 6D 70 6E 74 3E 3C 41 74  |s></POICmpnt><At|
0310  74 6E 64 6E 63 43 6E 74 78 74 3E 41 54 54 44 3C  |tndncCntxt>ATTD<|
0320  2F 41 74 74 6E 64 6E 63 43 6E 74 78 74 3E 3C 50  |/AttndncCntxt><P|
0330  4F 49 44 74 54 6D 3E 32 30 31 33 2D 31 32 2D 30  |OIDtTm>2013-12-0|
0340  36 54 31 33 3A 35 33 3A 34 39 2E 30 30 2B 30 32  |6T13:53:49.00+02|
0350  3A 30 30 3C 2F 50 4F 49 44 74 54 6D 3E 3C 2F 43  |:00</POIDtTm></C|
0360  6E 74 74 3E 3C 2F 44 61 74 61 53 65 74 3E 3C 2F  |ntt></DataSet></|
0370  53 74 73 52 70 74 3E                             |StsRpt>         |
```

The SHA256 digest of the *StatusReport* message body is:

```
0000  D2 ED A4 7B FE FF 0A E7 8A BD 7A 7D CE 6E AC 2A  |...{......z}.n.*|
0010  D3 82 05 46 5B BF B1 64 85 80 38 DF B6 3B 9B A5  |...F[..d..8..;..|
```

Applying the padding process for the digital signature, the block result is dumped below:

```
0000  00 01 FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0010  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0020  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0030  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0040  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0050  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0060  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0070  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0080  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
0090  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
00A0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
00B0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  |................|
00C0  FF FF FF FF FF FF FF FF FF FF FF FF 00 30 31 30  |.............010|
00D0  0D 06 09 60 86 48 01 65 03 04 02 01 05 00 04 20  |...`.H.e....... |
00E0  D2 ED A4 7B FE FF 0A E7 8A BD 7A 7D CE 6E AC 2A  |...{......z}.n.*|
00F0  D3 82 05 46 5B BF B1 64 85 80 38 DF B6 3B 9B A5  |...F[..d..8..;..|
```

After encryption by the private key of $K_{POI\text{-}Sign}$, we have the digital signature of the *StatusReport* message body:

```
0000  88 CF CD B0 F9 C4 EE 5E DD 6F BF 98 BA 09 56 40  |.......^.o....V@|
0010  FE 9A BC F3 5C 98 25 22 DD 31 4B 32 D1 84 6E 85  |....\.%".1K2..n.|
0020  A0 A4 D2 BC 88 D5 48 3C 76 BD A6 A5 E7 E3 B7 D6  |......H<v.......|
0030  CB DA 91 51 63 62 D3 26 27 A9 2F A7 91 EF FB E1  |...Qcb.&'./.....|
0040  A4 CE 7B 58 D5 55 00 8E 48 BE 66 55 8F EB 12 1A  |..{X.U..H.fU....|
0050  B9 C6 E2 95 C2 BA 49 8D 6B D3 78 B2 68 AC C0 7E  |......I.k.x.h..~|
0060  7E 7F 95 BB 5D 7B 03 EA DC D4 1D ED 81 38 80 21  |~...]{.......8.!|
0070  F5 54 D6 41 58 C8 BD 80 4E 0A B6 05 0D 49 DC 0E  |.T.AX...N....I..|
0080  45 65 54 76 69 41 FC 4C 4A FF 26 5C 24 F0 77 BA  |EeTviA.LJ.&\$.w.|
0090  A9 09 97 F5 7C 95 22 B7 01 CE 21 82 47 07 98 92  |....|."...!.G...|
00A0  48 9D F9 DE D1 E7 0B 05 43 66 CE 0D B4 3F B8 3D  |H.......Cf...?.=|
00B0  BC 01 5D 79 72 60 7A C4 B2 06 DD 95 6E C9 73 0C  |..]yr`z.....n.s.|
00C0  4B 23 B1 22 B0 47 45 AB 06 10 27 10 1C 48 4B 09  |K#.".GE...'..HK.|
00D0  AF 3F 4E F5 FB 05 DB 2F 39 D6 C2 8D 41 11 02 28  |.?N..../9...A..(|
00E0  E5 DE D9 48 95 F7 97 15 D8 07 58 A9 31 FE 15 AB  |...H......X.1...|
00F0  D3 BC FE 00 1A 2A DC F0 74 42 17 BE 36 8D A3 15  |.....*..tB..6...|
```

2368 Inside the *SecurityTrailer*, the *SignedData* CMS data structure is presented in the table below:

Message Item	*Value*
SecurityTrailer	
SignedData	
ContentType	SignedData
DigestAlgorithm	
Algorithm	SHA256
EncapsulatedContent	
ContentType	PlainData
Certificate	308204833082026BA003020102020C2225A8FB00071293D4641C3C300D06092A 864886F70D01010B05003068310B300906035504060C0242453110300E060355 040A0C07455041534F72673126302406035504 0B0C1D546563686E6963616C20 43656E746572206F662045787065727469736531 1F301D06035504030C164550 41532050726F746F636F6C732054657374204341302A181332303133303431 38 3130323534362B303130301813323031383130303131383230303052B30313030 307A310B300906035504060C0246523110300E060355040A0C07455041534F72 673126302406035504 0B0C1D546563686E6963616C2043656E746572206F6620 45787065727469736531 31302F06035504030C28455041532050726F746F636F 6C205465737420436C69656E742041757468656E7469636174696F6E30820122 300D06092A864886F70D01010105000382010F003082010A0282010100C22511 390B85DB3990A27638B850616C18B11BDF78494B48B61F8F8D032225A8FB0007 1293D4641C3CDDE18D47337EB7381AC12976820FF5C0B321E4EDF88C9B8F1627 0E0FC6FAB470449BA70B947139551ABE326686F538C4F7F63A45FF4CB9E66470 00B28B791E1205ADB6ACDC29854698D90ACC3B6C84F0F8C2EFBEE4E3F9844BD7 9AB14C1F22376198C13BEAC560DDC835104176729C7E62FBF4EC350DE4D385C4 8D3EA40A90D7AA5838FAED3E3C760D19BB84D1997077C72331F3ADF050B41DB5 FFD19D129E88C75331DA13264BE4C2F0B0A0AA09F77EED2C801FAD239E8FE5D8 B43F10708FC3D6054B9156C5B55184F1A294DAB8F8267162BE9BB54867020301 0001A30F300D300B0603551D0F040403020780300D06092A864886F70D01010B 05000382020100540DB4CCCA78C5B72EC34D6A55EE7C152ED54409419E0B7BC7 83B8559557C02CCA5E81B6CCA854A36250ADCA0CD55C96F42F019799B5A100C9 72D3F2411CB2676300F1B09E46AE4F293A24CB71EEA5467CB91933713E556FFC C0B558DA344FF4F8AB30A2F803BD97BB568100BAC6B6FAE884F831BF855C4EE8 23FE3BAC3BA2D8B615F62C1C1685B9BC59DFCBE1CFBDFDB29F3773FD46685688 BF656670F5BB9CE56B029E36E7291629DE69FA858367619D8DE4FB9F08608518 85A42894ADC97DCB51D4CEBF9F52083DD511371B157E3D16F93469EED0B7FF01 BC137D5065E266A8EA3C82999EF36263A863ED5FE22A69E4874FDF41A19FA457 B12CF6A52B08F73BD3BD9C2FD13352ECEE4EEF6323826BF72440FC149EBD5891 A8D6D0E5DA50547708525CA4021B51059B52B50E61B176C1F962AA7AC2809934 31DD5BF3D6C146ADBA762B3E6729F17FA639D98D5CBFDCAE556A2FC0B23754E4 91F97BF17A18D842A87F8DE4FBA58B56517213BC59C512D4F0447F0C197B3878 5A457E0A0E7DD44806C4BA16F811B7A25024791ED742E74392C9D4BABA754F09 B61DD8EC2ABBF6737E492BBC37185072AC9EBEA3DEF2FBD56E836B88D0809F96 A4B2ACA1A5B59D198F94990BA4D2A1B50CF64C5E8391D6DCADB58C9E074E608D 7D012309A92FFDCEFD96CDAEA4F6BE5E572A20161C3D6FD838FFAE966BB2C671 E7C836FB369C28
Signer	
SignerIdentification	
IssuerAnd-SerialNumber	
Issuer	
RelativeDistin-guishedName	
AttributeType	CountryName
AttributeValue	BE
RelativeDistin-guishedName	
AttributeType	OrganisationName
AttributeValue	EPASOrg
RelativeDistin-guishedName	
AttributeType	OrganisationUnitName
AttributeValue	Technical Center of Expertise

RelativeDistinguishedName	
AttributeType	CommonName
AttributeValue	EPAS Protocols Test CA
SerialNumber	2225A8FB00071293D4641C3C
DigestAlgorithm	
Algorithm	SHA256
SignatureAlgorithm	
Algorithm	SHA256WithRSA
Signature	88CFCDB0F9C4EE5EDD6FBF98BA095640FE9ABCF35C982522DD314B32D1846E85 A0A4D2BC88D5483C76BDA6A5E7E3B7D6CBDA91516362D32627A92FA791EFFBE1 A4CE7B58D555008E48BE66558FEB121AB9C6E295C2BA498D6BD378B268ACC07E 7E7F95BB5D7B03EADCD41DED81388021F554D64158C8BD804E0AB6050D49DC0E 456554766941FC4C4AFF265C24F077BAA90997F57C9522B701CE218247079892 489DF9DED1E70B054366CE0DB43FB83DBC015D7972607AC4B206DD956EC9730C 4B23B122B04745AB061027101C484B09AF3F4EF5FB05DB2F39D6C28D41110228 E5DED94895F79715D80758A931FE15ABD3BCFE001A2ADCF0744217BE368DA315

The XML encoded structure of the *StatusReport* message is:

```
<?xml version="1.0" encoding="UTF-8"?>
<Document xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="urn:iso:std:iso:20022:tech:xsd:catm.001.001.06">
 <StsRpt>
    <Hdr>
       <DwnldTrf>false</DwnldTrf>
       <FrmtVrsn>6.0</FrmtVrsn>
       <XchgId>003</XchgId>
       <CreDtTm>2013-12-06T13:53:55.00+02:00</CreDtTm>
       <InitgPty>
          <Id>66000001</Id>
          <Tp>OPOI</Tp>
          <Issr>MTMG</Issr>
       </InitgPty>
       <RcptPty>
          <Id>epas-keyDownload-TM1</Id>
          <Tp>MTMG</Tp>
       </RcptPty>
    </Hdr>
    <StsRpt>
       <POIId>
          <Id>66000001</Id>
          <Tp>OPOI</Tp>
          <Issr>MTMG</Issr>
       </POIId>
       <TermnlMgrId>
          <Id>epas-keyDownload-TM1</Id>
          <Tp>MTMG</Tp>
       </TermnlMgrId>
       <DataSet>
          <Id>
             <Tp>STRP</Tp>
             <CreDtTm>2013-12-06T13:53:55.00+02:00</CreDtTm>
          </Id>
          <Cntt>
             <POICmpnt>
                <Tp>TERM</Tp>
                <Id>
                   <ItmNb>1</ItmNb>
                   <PrvdrId>EPASVendor001</PrvdrId>
                   <Id>Counter Top E41</Id>
                   <SrlNb>7825410759</SrlNb>
                </Id>
             </POICmpnt>
             <POICmpnt>
```

```
            <Tp>APLI</Tp>
            <Id>
               <ItmNb>1.1</ItmNb>
               <PrvdrId>EPASVendor001</PrvdrId>
            </Id>
            <Sts>
               <VrsnNb>1.01</VrsnNb>
            </Sts>
            <StdCmplc>
               <Id>SEPA-FAST</Id>
               <Vrsn>3.0</Vrsn>
               <Issr>CIR</Issr>
            </StdCmplc>
         </POICmpnt>
         <POICmpnt>
            <Tp>SCPR</Tp>
            <Id>
               <ItmNb>1.1</ItmNb>
               <PrvdrId>EPASVendor001</PrvdrId>
               <Id>SpecV1TestKey</Id>
            </Id>
            <Sts>
               <VrsnNb>2010060715</VrsnNb>
               <Sts>OPER</Sts>
            </Sts>
            <Chrtcs>
               <KeyChckVal>Tga32/eadwU=</KeyChckVal>
            </Chrtcs>
         </POICmpnt>
         <AttndncCntxt>ATTD</AttndncCntxt>
         <POIDtTm>2013-12-06T13:53:49.00+02:00</POIDtTm>
      </Cntt>
   </DataSet>
</StsRpt>
<SctyTrlr>
   <CnttTp>SIGN</CnttTp>
   <SgndData>
      <DgstAlgo>
         <Algo>HS25</Algo>
      </DgstAlgo>
      <NcpsltdCntt>
         <CnttTp>DATA</CnttTp>
      </NcpsltdCntt>
      <Cert>
         MIIEgzCCAmugAwIBAgIMIiWo+wAHEpPUZBw8MA0GCSqGSIb3DQEBCwUAMGgxCzAJBgNVBAYMAkJFMR
         AwDgYDVQQKDAdFUEFTT3JnMSYwJAYDVQQLDB1UZWNobmljYWwgQ2VudGVyIG9mIEV4cGVydGlzZTEf
         MB0GA1UEAwwWRVBBUyBQcm90b2NvbHMgVGVzdCBDQTAqGBMyMDEzMDQxODEwMjU0NiswMTAwGBMyMD
         E4MTAwMTE4MjAwNSswMTAwMHoxCzAJBgNVBAYMAkZSMRAwDgYDVQQKDAdFUEFTT3JnMSYwJAYDVQQL
         DB1UZWNobmljYWwgQ2VudGVyIG9mIEV4cGVydGlzZTExMC8GA1UEAwoRVBBUyBQcm90b2NvbCBUZX
         N0IENsaWVudCBBdXRoZW50aWNhdGlvbjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMIl
         ETkLhds5kKJ2OLhQYWwYsRvfeElLSLYfj40DIiWo+wAHEpPUZBw83eGNRzN+tzgawSl2gg/1wLMh5O
         34jJuPFicOD8b6tHBEm6cLlHE5VRq+MmaG9TjE9/Y6Rf9MueZkcACyi3keEgWttqzcKYVGmNkKzDts
         hPD4wu++5OP5hEvXmrFMHyI3YZjBO+rFYN3INRBBdnKcfmL79Ow1DeTThcSNPqQKkNeqWDj67T48dg
         0Zu4TRmXB3xyMx863wULQdtf/RnRKeiMdTMdoTJkvkwvCwoKoJ937tLIAfrSOej+XYtD8QcI/D1gVL
         kVbFtVGE8aKU2rj4JnFivpu1SGcCAwEAAaMPMA0wCwYDVR0PBAQDAgeAMA0GCSqGSIb3DQEBCwUAA4
         ICAQBUDbTMynjFty7DTWpV7nwVLtVECUGeC3vHg7hVlVfALMpegbbMqFSjYlCtygzVXJb0LwGXmbWh
         AMly0/JBHLJnYwDxsJ5Grk8pOiTLce6lRny5GTNxPlVv/MC1WNo0T/T4qzCi+AO9l7tWgQC6xrb66I
         T4Mb+FXE7oI/47rDui2LYV9iwcFoW5vFnfy+HPvf2ynzdz/UZoVoi/ZWZw9buc5WsCnjbnKRYp3mn6
         hYNnYZ2N5PufCGCFGIWkKJStyX3LUdTOv59SCD3VETcbFX49Fvk0ae7Qt/8BvBN9UGXiZqjqPIKZnv
         NiY6hj7V/iKmnkh0/fQaGfpFexLPalKwj3O9O9nC/RM1Ls7k7vYyOCa/ckQPwUnr1YkajW0OXaUFR3
         CFJcpAIbUQWbUrUOYbF2wfliqnrCgJk0Md1b89bBRq26dis+Zynxf6Y52Y1cv9yuVWovwLI3VOSR+X
         vxehjYQqh/jeT7pYtWUXITvFnFEtTwRH8MGXs4eFpFfgoOfdRIBsS6FvgRt6JQJHke10LnQ5LJ1Lq6
         dU8Jth3Y7Cq79nN+SSu8NxhQcqyevqPe8vvVboNriNCAn5aksqyhpbWdGY+UmQuk0qG1DPZMXoOR1t
         yttYyeB05gjX0BIwmpL/3O/ZbNrqT2vl5XKiAWHD1v2Dj/rpZrssZx58g2+zacKA==
      </Cert>
      <Sgnr>
         <SgnrId>
            <IssrAndSrlNb>
               <Issr>
```

```
                  <RltvDstngshdNm>
                        <AttrTp>CATT</AttrTp>
                        <AttrVal>BE</AttrVal>
                  </RltvDstngshdNm>
                  <RltvDstngshdNm>
                        <AttrTp>OATT</AttrTp>
                        <AttrVal>EPASOrg</AttrVal>
                  </RltvDstngshdNm>
                  <RltvDstngshdNm>
                        <AttrTp>OUAT</AttrTp>
                        <AttrVal>Technical Center of Expertise</AttrVal>
                  </RltvDstngshdNm>
                  <RltvDstngshdNm>
                        <AttrTp>CNAT</AttrTp>
                        <AttrVal>EPAS Protocols Test CA</AttrVal>
                  </RltvDstngshdNm>
               </Issr>
               <SrlNb>IiWo+wAHEpPUZBw8</SrlNb>
            </IssrAndSrlNb>
         </SgnrId>
            <DgstAlgo>
               <Algo>HS25</Algo>
            </DgstAlgo>
            <SgntrAlgo>
               <Algo>ERS2</Algo>
            </SgntrAlgo>
            <Sgntr>
               iM/NsPnE7l7db7+YuglWQP6avPNcmCUi3TFLMtGEboWgpNK8iNVIPHa9pqXn47fWy9qRUWNi0
               yYnqS+nke/74aTOe1jVVQCOSL5mVY/rEhq5xuKVwrpJjWvTeLJorMB+fn+Vu117A+rc1B3tgT
               iAIfVU1kFYyL2ATgq2BQ1J3A5FZVR2aUH8TEr/Jlwk8He6qQmX9XyVIrcBziGCRweYkkid+d7
               R5wsFQ2bODbQ/uD28AV15cmB6xLIG3ZVuyXMMSyOxIrBHRasGECcQHEhLCa8/TvX7BdsvOdbC
               jUERAijl3tlIlfeXFdgHWKkx/hWr07z+ABoq3PB0Qhe+No2jFQ==

            </Sgntr>
      </Sgnr>
   </SgndData>
 </SctyTrlr>
</StsRpt>
</Document>
```