Smart Metering Implementation Programme

Great Britain Companion Specification (GBCS)

Security

Version 0.8.1: Release Note
28 November 2014

Devices in Scope of GBCS

- ESME

- GSME

- CH-CHF

- CH-GPF

- PPMID

- Type-2 Devices(IHD)

Objective of GBCS

- The purpose of this GBCS, and related documents, is to specify the single, consistent technical implementation in sufficient detail to achieve operational interoperability of Devices.

- These include standards relating to *DLMS COSEM*, *ZSE*, *ASN.1*, *NSA Suite B cryptography* and *X.509 related IETF RFCs*. The GBCS does not duplicate what is laid out in such standards but rather provides references to them.

Key Terms Used in GBCS

- **Remote Party**= Organization communicating with devices are called Remote Party

- **Messages**= "end-to-end" & "Unicast"

  -> Identify Sender & Intended Recepient

  -> would be commands,responses or Alerts

  ->Message to/from remote party is treated as remote party message

  ->Messages between Devices are called HAN Only Messages

  <u>The GBCS specifies how all such Messages are constructed and related processing performed</u>

Cont.

- Messages are classified in two categories,

  a)HAN Only Message,

  b)Remote Party Message

- Known Remote Party(KRP) & Unknown Remote Party(URP)

- Commands requiring a Response to an Unknown Remote Party shall always be sent to the Device by the Device's Access Control Broker(ACB)

- Type-2 Devices shall not be required to support any Remote Party Messages

Terminology

- **Numbers:**

    a) if no prefix, it is a decimal number(base 10),

    b) if prefix=0x, it is a hexadecimal number(base 16),

    c) if prefix=0b, it is a binary number(base 2)

- **Bit Numbering**: Uses "LSB0" scheme

- **Octet & Bytes**: refer unit of 8 bits of digital information

- **Tag**: always used in the sense it is meant in encoding standards,such as DER

- **MAC**: always used to mean Message Authentication Code,which is a cryptographic checksum on data

- **Concatenation**: X || Y shall mean the concatenation of the two octet strings X and Y

Cont.

- **Encoding of Variable length unsigned variable**

  ->if *0<X<128*, then Encoding(X) is a single octet whose value is X,

  -> if *128<= X <32,768*, then Encoding(X) is a an octet string composed of the concatenation 0x82 || Y, where Y is two octets in length and has a value equal to the two's complement representation of the value X,

  ->if *32,768<= X <8,388,608*, then Encoding(X) is a an octet string composed of the concatenation 0x83 || Y, where Y is three octets in length and has a value equal to the two's complement representation of the value X.

- **Len(Encoding(X))** shall be the length in octets of Encoding(X), so shall be either 1 (X<128), 3 (128<= X <32768) or 4 (32,768<= X <8,388,608)

Cont.

- **Generalized Time**:

    -> The GeneralizedTime ASN.1 type used in this GBCS shall be a UTC(Corordinated Universal Time) Time with a resolution of one second.

Security

- Why Security is needed here?

- Security Provisions that are common across remote party messages,

    ->Identifiers,Counters & Protection Against Replay,

    ->Security Credentials,

    ->Cryptographic Primitives & their Usage

- Term used in this GBCS,

    -> Remote Party Originator Counter,Device Originator Counter

    ->Supplementary Remote Party Counter,

    -> Supplementary Originator Counter,

    ->Execution Counter

Security for Remote Party Message

- Apply only to all Remote Party Messages

    1) Identifiers,Counters & Protection Against Replay,

    -> Identifiers= Entity Identifier of smart metering entities,shall be octet string length 8 and unique across GB smart metering.

Message Type	Business Originator ID	Business Target ID
Command	Entity Identifier for the KRP which is requesting execution of this Command	Entity Identifier for the Device that the Remote Party wants to action the Command
Response	The Entity Identifier for the Device. This is always the same as the Business Target ID supplied in the corresponding Command	The Business Originator ID provided in the corresponding Command.
Alert	The Entity Identifier for the Device	The Entity Identifier for the KRP to which the Alert is to be addressed

Cont.

- Originator Counter

  ->A Remote Party Message shall include an Originator Counter, which shall be octet string of length 8 whose contents shall be set and read as an unsigned 64-bit integer.

- If Remote Party is required to generate an Originator Counter, the Remote Party shall ensure that,

  -> value is strically numerically greater than any previous originator counter value it has provided for use in any previous command,

  ->the 32 least significant bits shall not all have the value 0b0 unless the Command is a Prepayment Top Up Command.

Message	Responsibility for generating the Originator Counter
Command	The Known Remote Party identified by the Business Originator ID in the Command.
Response	The Originator Counter shall have the same value as in the corresponding Command.
Alert	The Device generating the Alert.

Cont.

- Message Identifier

  -> A Message Identifier shall be the concatenation of,

  Business Originator ID || Business Target ID || CRA Flag || Originator Counter

  -> All Message Shall include Message Identifier

- Additional Counters and Identifiers

  -> if B.O.I. is set to be that of ACB & Message code is listed in the 'Use Case reference' worksheet of the Mapping Table as 'Supplementary Remote Party Data required' then,

    -> Supplementary Remote Party ID,

    -> Supplementary Remote Party Counter

- Protection Against Replay Mechanism

  -> Device shall have all Execution Counters initially set to zero at manufacture & have capabilities to store an Originator Counter value for each Remote Party Role

Cont.

2) Security Credentials

    -> Four Kind of Security Credentials shall be processed by Device,

    a) Device Certificate,

    b) Organization Certificate (For KRP),

    c) Organization Certificate (For URP),

    d) Certification Authority Certificates

3) Device Security Credentials

    ->If DeviceType is gSME,eSME,CHCHF or CHGPF, these device shall have capacity to store and use securely 4 private keys:

        ->For Key Agreement: Current & Pending Private Keys
        ->For Digital Signing: Current & Pending Private Keys

    ->If DeviceType is Type-1 or HCALCS or PPMID,these device shall have capacity to store and use securely 2 private keys:

        ->For Key Agreement: Current Private Key
        ->For Digital Signing: Current Private Key

Cont.

- These stores shall be reffered to as Private Key Cells

- Only Relevant current private key shall be used for cryptographic protection

- Public-Private Key Pair shall have been generated if device holds private key that is to be used for <u>Key Agreement & Digital Signature</u>

- If Device Support Remote Party's message, the device shall have two Trust Anchor Cells(TACs) to store two certificates,

  a) TAC for storing Device certificate where key usage=KeyAgreement,
  b) TAC for storing Device certificate where key usage=DigitalSignature

  ->Both certificate's *hwSerialNum* fields have a value the same as the Device's *Entity Identifier*

  ->Each Device Certificate's *keyUsage* field has the same value as the TAC in which it is placed

Cont.

4) Remote Party Security Credentials

- A Device shall only action a Remote Party Command where,

  -> the KRP identified by the command has, according to the Security Credentials held on the Device, a Remote Party Role which, according to the Mapping Table,

  ->the Cryptographic Protections in the command instance received by the Device have been verified

- To enable this, Security Credentials relating to the Remote Parties,

  ->shall be held in Trust Anchor Cells on the Device

  ->shall act as the corresponding Trust Anchors

Cont.

5) Required TACs & Related

   Device Requirements

			Type of Device (✓ = is required; empty = is not required)					
			ESME	GSME	CH (CHF)	CH (GPF[B])	HCALCS	PPMID
		deviceType value(s)	1	0	2	3	4	5
TrustAnchorCellIdentifier								
remotePartyRole	**keyUsage**	**cellUsage**						
Root	keyCertSign	Management	✓	✓	✓	✓	✓	✓
Recovery	digitalSignature	Management	✓	✓	✓	✓	✓	✓
Supplier	digitalSignature	Management	✓	✓		✓	✓	
Supplier	keyAgreement	Management	✓	✓		✓		
Supplier	keyAgreement	prePaymentTopUp	✓	✓				
networkOperator	digitalSignature	Management	✓			✓		
networkOperator	keyAgreement	Management	✓			✓		
accessControlBroker	digitalSignature	Management			✓			✓
accessControlBroker	keyAgreement	Management	✓	✓	✓	✓	✓	✓

Cont.

- Specific Trust Anchor Cell shall be identified in this GBCS using the notation **{remotePartyRole, keyUsage, cellUsage}**. For example {supplier, digitalSignature, management} shall refer to the Trust Anchor Cell that holds the Device's Supplier Digital Signing Security Credentials, so including the Supplier's:

  -> Entity Identifier,
  -> Remote Party Role,
  -> Digial Signing Public Key

- If a Device supports the processing of Remote Party Messages, that Device:

  -> shall support the processing of the *Update Security Credentials Command* or *Provide Security Credentials Command* & shall not allow execution of any Remote Party Command other than these two.

Cont.

6) Usage of Public Key in each TAC

TrustAnchorCellIdentifier			Usage of the Public Key in the Trust Anchor Cell
remotePartyRole	keyUsage	cellUsage	
Root	keyCertSign	management	Used only in Certification Path Validation to check that Certification Authority Certificates and Certificates related to change of root credentials were validly issued
Recovery	digitalSignature	management	Used only to verify recovery's signature on Update Security Credentials Commands addressed to the Device
Supplier	digitalSignature	management	Used to verify the supplier's signature on Critical Commands the supplier has addressed to the Device
Supplier	keyAgreement	management	Used in applying MACs to Alerts and Responses addressed to the supplier, where they are not Critical Used in unencrypting encrypted data in Commands from the supplier and in encrypting data

TrustAnchorCellIdentifier			Usage of the Public Key in the Trust Anchor Cell
remotePartyRole	keyUsage	cellUsage	
			in Alerts and Responses addressed to the supplier
Supplier	keyAgreement	prePaymentTopUp	Used to check the supplier MAC on prepayment top up Commands. The supplier can decide whether this is the same key as the Key Agreement key used for other purposes
networkOperator	digitalSignature	management	Used to check the signature of the networkOperator on Critical Commands the networkOperator has sent to the Device. This only equates to Update Security Credentials Commands
networkOperator	keyAgreement	management	Used in applying MACs to Alerts and Responses addressed to the networkOperator, where they are not Critical

Used in encrypting data in Responses addressed to the networkOperator |
accessControlBroker	digitalSignature	management	Used to verify the accessControlBroker's signature on Commands addressed to the Device
accessControlBroker	keyAgreement	management	Used in checking the accessControlBroker MAC on Commands received and to calculate the MAC for Responses addressed to the accessControlBroker
transitionalCoS	digitalSignature	management	Used only to check transitionalCoS's signature on Update Security Credentials Commands received by the Device
wanProvider	digitalSignature	management	Used by the Communications Hub (CHF) to verify the wanProvider's signature on Critical Commands addressed to the Communications Hub

Cont.

7) Cryptographic Verification of Remote Party Command

- Message Authentication Codes (MAC)

  ->If Command=Prepayment Topup,supplier MAC shall be varified using public key in TAC{supplier,keyagreement,prepaymenttopup},along with device's key agreement private key

  ->All other MAC in command shall be verified using the public key in the TAC{acb,keyagreement,management},along with device's key agreement private key

- Signature

  ->If command has digital signature,the device shall identify remote party role which can sign the command according to the message code identified in the Mapping Table

  ->If there is only one remote party role identified, then the signature shall be verified using the public key in TAC {the identified remote party role,digital certificate,management}

Cont.

-> If there is more than one Remote Party Role so identified, the Device shall use the Business Originator ID in the Command to identify the Trust Anchor Cell(s) where:

->keyusage=DigitalSignature

->cellusage=management, &

->existingSubjectUniqueID = the Business Originator ID in the Command

->If there is only one Trust Anchor Cell so identified, then the signature shall be verified using the Public Key in that Trust Anchor Cell.

->If there is more than one Trust Anchor Cell so identified the Device shall attempt to verify the Digital Signature using each Trust Anchor Cell identified.These attempts shall be according to the following precedence,

-> supplier, ->wanProvider, ->networkOperator, ->acb

Cont.

8) Certification Path Validation

- Access Control Broker (ACB) Requirements

->Before ACB to Device MAC (ACB SMD MAC) calculation, the ACB shall undertake Certification Path Revocation(CRL) validation for any organization certificate in command,

->either by using the algorithm specified in IETF RFC 5280(https://www.ietf.org/rfc/rfc5280.txt), or

->by using functionality equivalant to the external behaviour resulting from algorithm

->Only if the CRL Validation is successful shall the Access Control Broker calculate the ACB-SMD MAC

Cont.

- Device Requirements (apply to only *Update Security Credentials*)

    ->If Device has sucessfully completed all required authenticity & integrity checks, the device shall undertake either,

    >->Certification Path Validation, including time checks; or

    >->Certification Path Validation, excluding time checks

    ->the Trust Anchor information shall be in the *root* Security Credentials held on the device

    ->If the device's certificate path validation does not confirm the required path validaty,then the device shall undertake no further processing of the command ,except for the issuance of a Response notifying that the command was unsucessful

9) DLMS Client and Server

    ->The Access Control Broker shall perform the role of DLMS COSEM client in relation to the DLMS COSEM Application Associations, and the Device shall perform the role of DLMS COSEM server.

Cryptographic Primitives & their Usage

- In relation to any Remote Party Message, Smart Metering Entities shall:

  ->use **SHA-256**, as specified in FIPS 180-4, as the Hash function

  ->use the **AES-128** cipher, as specified in FIPS 197, as the block cipher primitive

  ->use the **Galois Counter Mode** (GCM) of operation as specified in NIST Special Publication 800-38D

  ->use the **GMAC** technique, based on the use of AES-128, for the calculation of Message Authentication Codes (MACs), as specified in NIST Special Publication 800-38D

  ->use, as the Digital Signature technique, **ECDSA** (as specified in FIPS PUB 186-4)combination with the curve P-256 (as specified in FIPS PUB 186-4) and SHA-256 as the Hash function. Within Messages, Signatures shall be in the Plain Format

  ->use, to calculate the Shared Secret Z, the **Static Unified Model, C(0e, 2s, ECC CDH)** Key Agreement technique (as specified in NIST Special Publication 800-56Ar2 Save for the requirement to zeroize the Shared Secret) with:

    -> the Single-step Key Derivation Function (KDF) based on SHA-256

    ->the P-256 curve for the elliptic curve operations

Calculating unique shared secret key for remote party message

- If a Smart Metering Entity executes the KDF in relation to a Message instance, the OtherInfo field, shall be populated using the value of information provided from the Grouping Header

- The OtherInfo shall be in the Concatenation of:

    AlgorithmID || value of originator-system-title || length of transaction-id || value of transaction-id || value of recipient-system-title

    ->where AlgorithmID is for AES-GCM 128 & has a value 0x60857406080300(specified in green book)

    ->length of transaction-id is 0x09

Calculating the Initialization Vector for GCM and GMAC

- In relation to Remote Party Messages, Smart Metering Entities shall use a 96 bit Initialization Vector (IV) for the GCM and GMAC algorithms as defined in NIST Special Publication 800-8D. The IV shall be the concatenation of:

  FixedField || InvocationField

  ->where FixedField = the Entity Identifier of the Smart Metering Entity that is creating, or has created, the Cryptographic Protection,
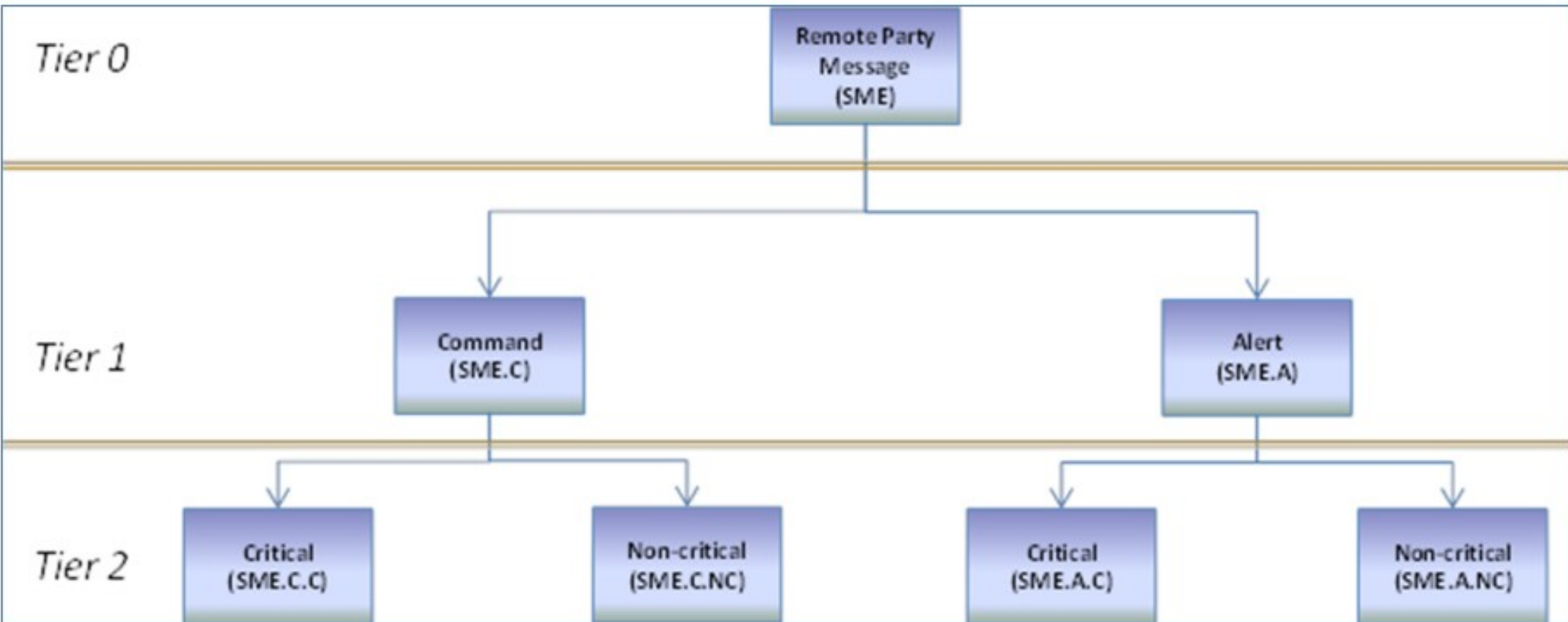
  ->InvocationField = 0x00000000

- The DLMS COSEM Authentication Key (AK), as defined in the Green Book, shall not be present.

- The bit length of the MAC shall be 96

Remote Party Message Construction,Protection & Verification

Introduction

- Common Message Structures

  ->All message constructed using aggregation structures

- Common Encryption & Decryption approach

- Message Categories

  ->the Message is a <u>Command, Response or Alert, and</u>

  ->the Message is a <u>Critical Message or not</u>

  ->Note that the 'Command' part of the hierarchy covers requirements for both the Command and the corresponding Response.

Message Categories

->A category which is derived from another category is called <u>subordinate message category</u>
->A category from which another category is derived is called <u>superordinate message category</u>

Common Message Processing Steps: Command Stages

Name of Stage	Summary of the stage	Responsible Smart Metering Entity
i. Command Construction	The Command is fully populated, apart from cryptographic fields	N/A The entity undertaking this phase is not known to the Device Although not apparent to the Device, the DSP's Transform Service would normally undertake such construction for DCC managed Devices
ii. Command Cryptographic Protection I	This stage is only needed where a Remote Party, other than the Access Control Broker, is required to add Cryptographic Protection to the Command. So for digital signing of Critical Commands only	Known Remote Party
iii. Command Cryptographic Protection II	The Access Control Broker adds its Cryptographic Protection to the Message. This is by way of the ACB adding a MAC	Access Control Broker
iv. Command Authenticity and Integrity Verification	The Device undertakes the range of checks needed, including those to ensure authenticity of the sender and integrity of the Message. This includes checking the Identifiers and Counter in the Command and	Device

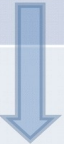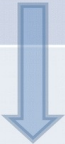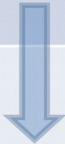| Name of Stage	Summary of the stage	Responsible Smart Metering Entity
	verifying the Access Control Broker's MAC	

Command Stages for Response

Name of Stage	Summary of the stage	Responsible Smart Metering Entity
v. Response Construction	The Response is fully populated by the Device, apart from cryptographic fields	Device
vi. Response Cryptographic Protection	The Device adds the required Cryptographic Protection to the Response	Device
vii. Response Recipient Verification	The Remote Party (Parties) can undertake the range of checks, including those to ensure authenticity of the sender and integrity of the Message	Remote Party named in the Response

Command Stages for Alert

Name of Stage	Summary of the stage	Responsible Smart Metering Entity
viii. Alert Construction	The Alert is fully populated by the Device, apart from cryptographic fields	Device
ix. Alert Cryptographic Protection	The Device adds the required cryptographic fields to the Alert	Device
x. Alert Recipient Verification	The Remote Party (Parties) can undertake the range of checks, including those to ensure the authenticity of the sender and integrity of the Message	Remote Party named in the Alert

The generic processing applied to Commands and their Responses (in relation to integrity, authenticity and non-repudiation) in a Message Category

	Command Construction	Command Cryptographic Protection I	Command Cryptographic Protection II	Command Authenticity and Integrity Verification	Response Construction	Response Cryptographic Protection	Response Recipient Cryptographic Verification
Responsible Party	*Not known to Device*	*Known Remote Party*	*Access Control Broker*	*Smart Metering Device*	*Smart Metering Device*	*Smart Metering Device*	*Remote Party as named in the response*
1 – Command (SME.C)	Commands contain sender ID, recipient ID and a Counter	-	Applies a MAC for the Device	Device checks Identifiers, checks the Counter and validates the MAC	Responses contain sender ID, recipient ID and a Counter	-	Can check Identifiers and the Counter
2 – Critical (SME.C.C)		Digitally signed		*PLUS:* Verifies digital signature		*PLUS:* Digitally signed	*PLUS:* Can verify digital signature

1 – Command (SME.C)	Commands contain sender ID, recipient ID and a Counter	-	Applies a MAC for the Device	Device checks Identifiers, checks the Counter and validates the MAC	Responses contain sender ID, recipient ID and a Counter	-	Can check Identifiers and the Counter
2 – Non-critical (SME.C.NC)		-				*PLUS:* Applies a MAC for the KRP	*PLUS:* Can verify the MAC

The generic processing applied to Alerts in a Message Category

	Alert Construction	Alert Cryptographic Protection	Alert Recipient Cryptographic Verification
Responsible Party	*Smart Metering Device*	*Smart Metering Device*	*Remote Party as named in the response*
1 – Alert (SME.A)	Alerts contain sender ID, recipient ID and a Counter	-	Can check Identifiers and the Counter
2 – Critical (SME.A.C)	⬇	Digitally signed	*PLUS:* Can verify digital signature
1 – Alert (SME.A)	Alerts contain sender ID, recipient ID and a Counter	-	Can check Identifiers and the Counter
2 – Non-critical (SME.A.NC)	⬇	Applies a MAC for the KRP	*PLUS:* Can verify the MAC

Common processing stages and requirements for Devices operated through the DCC

- For DCC managed Devices, the DSP would operate the services that provide (1) Access Control Broker, (2) Transform Service and (3) Transitional Change of Supplier.

  ->Sequence diagram for processing Critical Remote Party Commands and Responses ---> See note_1 document, Page1

  ->Sequence diagram for processing non Critical Remote Party Commands and Responses ---> See note_1 document,Page 2

  -> Sequence diagram for processing Critical Remote Party Alerts---> See note_1 document, Page3

Cryptography sequence

To understand the flow of message/key encryption and decryption , lets take an example,

-> Sender=A, Receiver=B, Message=M

1) Sender A has a message, M, to send to B. A computes its hash, H(M) and encrypts it with its own private key: Ea(H(M)). This is its Signature.

2) Secrecy of the message is important in this example, so A will encrypt the signed message with a symmetric algorithm using a randomly generated key, K.

-> The encrypted signed message is EK({M,Ea(H(M))}).

3) Now A has to enable only B to be able to decrypt this message, so she encrypts the key, K, with Bob's public key: EB(K). Finally, A sends out the complete message: { EK({M,Ea(H(M))}), EB(K) }.

4) B will decrypt the key, k, by using its private key and then decrypt encrypted signed message.

5) Now B will compute Hash of M,H(M), and decrypt encrypted Hash in received message with A's Public key

6) B will now compare generated Hash and received hash.

7) If both Hash are equal then,message is non-altered and processed. If not equal then message will be discarded

Example of Encryption and Decryption by using Symmetric Key

- Suppose we have message to be encrypted: "Hello all How are you" and symmetric key=6552 .

- By using transpositional algorithm,we can encrypt this message as,

- Total length of message=17 and length of Key=4, Blocks=L(M)/L(Key)=5(ceailing value)

- Lets arrange message in raw, fill remaining field With mark of 'X'

6	5	5	2
H	E	L	L
O	A	L	L
H	O	W	A
R	E	Y	O
U	X	X	X

- Now start to write message column wise, from lowest key number to highest. It will have the content like,

  LLAOXEAOEXLLWYXHOHRU->encrypted message

- We can decrypt the excrypted message by using same key and reverse process of encryption.

Public-Private Key Pair Generation Method

- For **Key Agreement**, NSA's 'Suite B Implementer's Guide to NIST SP 800-56Ar2' using the 'Key Pair Generation Using Extra Random Bits' method.

    -> specifies key-establishment schemes based on the discrete logarithm problem over finite fields and elliptic curves, including several variations of Diffie-Hellman and Menezes-QuVanstone(MQV) key establishment schemes.

    -> http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf

- For **Digital Signature**, NSA's 'Suite B Implementer's Guide to FIPS 186-3 (ECDSA), February 3, 2010' using the 'ECC Key Pair Generation Using Extra Random Bits' method.

    -> Used elliptic curve cryptography to authenticate security certificates

    ->https://www.nsa.gov/ia/_files/ecdsa.pdf

Keywords

- NSA: National Security Agency(Intelligent Organization of US Govt.)

- NIST: National Institute of Standards and Technology(A non-regulatory federal agency under the Department of Commerce headquartered in Gaithersburg, MarylandA NIST certification is important because it supports and develops measurement standards for a particular service or product)

- NIST SP: NIST Special Publication(Security and Privacy Controls for Federal Information Systems and Organizations)

- FIPS: Federal Information Processing Standards (Are a set of standards that describe document processing, encryption algorithms and other information technology standards)

- ECDSA: Elliptic Curve Digital Signature Algorithm (Used to Sign security certificate by using elliptic curve analogy)

- ECC: Elliptic Curve Cryptography

- IETF RFC: A Request for Comments (RFC) is a publication of the Internet Engineering Task Force (IETF) and the Internet Society, the principal technical development and standards-setting bodies for the Internet.

- IETF RFC5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

- GMAC: Galloic Counter Mode Message Authentication Code

- ECDSA(r, s): An ECDSA digital signature, where r and s are the digital signature components

- Variant Message:A Message which include security credentials and Prepayment Top Up related messages

- DCC: Data & Communication Company