STANDARD TRANSFER SPECIFICATION STS EDITION 2

IEC62055-41: 2018
Edition3

STS EDITION 2

IEC62055-41: 2018 published 21 May 2018

State of the art security

2, 3, 4 KCT – allows transfer of SGC

DLMS/COSEM via VTC port

Currency support for all utility types

Higher credit resolution for gas and time

COMPANION SPECIFICATIONS

The following companion specifications are withdrawn as of 22 May 2018:

- STS202-1 : Currency
- STS202-2 : Group coded PAN
- STS202-3 : EA and DKGA

ENCRYPTION ALGORITHMS

- New encryption algorithm (EA11 – Misty 1)
  - 128bit as opposed to 64 bit legacy system
  - Can only be used with DKGA04
- STS6 protocol for HSM – new protocol required due to increased functionality
- Legacy EA07 still supported
- Removed support for DES for EA09 and TDES for EA03

KEYCHANGE TOKENS

- Added support for three keychange token set
  - Allows for the transfer of SGC to the payment meter
- EA=11 (Misty1) will have 4 keychange tokens due to the longer key length of 128 bits
- Support for legacy keychange pair maintained

CURRENCY

- Added support for currency tokens
  - *Electricity*
  - *Water*
  - *Gas*
  - *Time*
- Class 0 - Subclasses 4 – 7
- 10^{-5} base units resolution to allow for a large range of currency values

DLMS/COSEM

- Support added for inclusion of STS tokens in the DLMS/COSEM suite
  - STS token transfer defined in DLMS Blue Book
  - Covered by STS101-2 and STS201-2
- VTC08 added to support DLMS/COSEM

CREDIT TRANSFER RESOLUTION

All utility credit transfers now at a higher resolution

- Electricity (0.1 kWh – current)
- Water (0.1m^3)
- Gas (0.1m^3)
- Time (0.1 min)

SECURE MODULE API

- STSA acquired all rights to the API documents
- Conversion to open standards by June 2018
- Opens the market for developers of security modules
- Document numbers:
  - STS600-8-1 to STS600-8-6
  - These cover all current and new SM’s

Secure Module API

- New protocol for security modules
- Owned by the STSA – open standard
- allows for key expiry and revocation
- Supports EA07 and EA11, DKGA02 and DKGA04
- Paves the way for other manufacturers of HSM devices to supply the industry
- Supports all the requirements for multiple base dates

KMC600 FEATURES

- Support for new algorithms (EA and DKGA)
- 192 bit key encryption
- Very secure key agreement scheme using Diffe-Helmann
- Key revocation, expiry, refresh
- Support for legacy algorithms and keyload files
- Support for multiple base dates

OTHER CHANGES

- Introduced token extension allowing for setting of meter parameters – STS202-5
- Added registers to STS201-1 to cater for this
- Introduced universal default key

THANK YOU

QUESTIONS?

CONTACT THE STS ASSOCIATION

STS Association Website:

https://www.sts.org.za/