Tel: +27 11 343 2000 | **Fax**: +27 11 442 5908 | **Email**: info@prism.co.za
Address: President Place, Johannesburg, South Africa

Introduction to STS and PrismToken

2018/12/12

Document number:	PR-D2-1060 Rev 1.4
Release date:	2018/12/12
Prepared by:	TrevorD
Copyright:	© 2020 Prism Payment Technologies
Synopsis:	Provides an introduction to the STS environment, the new STS6 standard, and Prism's PrismToken product.

Company Confidential

Disclaimer

Contents

1 Products in the STS environment

1.1 Prepaid meters

- Meters measure and control the supply of a resource (e.g. electricity, water, gas, time) to a customer. A meter is installed on the customer's supply line by the Utility that supplies the resource to the customer. Prepaid meters have a credit balance that decrements as the resource is consumed, and the meter cuts off the flow of the resource when the credit balance reaches zero.
- STS Meters are able to accept instructions (called "tokens") that alter the meter's credit balance or cause other technical changes in the meter.
- Tokens are created using a Vending Key. Each meter has a Supply Group Code (SGC) that identifies which Vending Key must be used to create a token that can be understood by the meter.Prism does not make meters.

1.2 Vending Systems

- A Vending System is able to create the instructions ("tokens") that alter the meter's credit balance; these tokens are usually printed on a receipt. A Vending System must use a Vending Key to create the token. Vending Keys are protected by peripheral hardware called a Security Module (SM). There is a central repository of Vending Keys called a Key Management Centre (KMC).
- The vending system must comply with various STS standards (e.g. IEC 62055-41, STS600-4-2, and others) and must be certified by the STS Association.A typical vending system includes: Point of Sale including payment acquisition and receipt printing; a database of the Utility's meters, their Point of Connection, and associated customer; arrears and debt collection; tariff support to translate currency-denominated purchases into resource units (e.g. kWh electricity); business rules applicable to vending; ability to issue STS tokens and manage STS vending keys; a transaction database, with support for reporting; reconciliation and settlement.
- Prism has developed the "TsmWeb-STS" and "Utility Vending System (UVS)" vending system products.

1.3 Key Management Centre (KMC)

- The Key Management Centre is a central repository for Vending Keys in the STS environment. Vending Keys are the digital secrets that protect STS instructions ("tokens") and prevent them from being forged. Each Vending Key is identified by a Supply Group Code (SGC) and a Key Revision Number (KRN).
- The KMC creates and stores keys on behalf of Utilities, and securely distributes those keys to Security Modules that are used by meter manufacturers (who inject keys into meters) and by vending systems (where they are used to create tokens).
- Prism has developed the "STS Key Management System" for the STSA, currently operated by Eskom.

1.4 Security Modules

- Security Modules are peripheral hardware that protects Vending Keys, allowing the keys to be used for specific purposes but protecting them against being copied. All keys in the STS ecosystem are protected by either a Security Module or a meter; keys are never allowed to be processed in software.

All Key Management Centres and Vending Systems require Security Modules to perform key-related operations, including creating STS tokens.

- Prism has developed the TSM500i with MCM/STS firmware for Key Management Centres.
- Prism has developed the TSM250 and TSM500i with STS firmware for Vending Systems. Two flavours of firmware are available:
    - STS/Legacy which supports IEC 62055-41 Ed 1 (2007) tokens and uses the legacy key management technique developed by Eskom; and
    - STS6 which supports IEC 62055-41 Ed 3 tokens and the STS600-4-2 key management standard, with vendor extensions for risk management.

2 Value proposition of STS

The core value of STS standards to Utilities is:

- Secure, vendor-neutral standard to transfer credit to prepayment meters.
- Unit-based or Currency-based credit.
- Compact token delivered via DLSM/COSEM, with offline backup channel.
- Keys & revenue protected by Security Module.

3 STS6

3.1 What is it?

"STS6" is a moniker referring to the next generation of STS standards, including:

- The STS600-4-2 key management standard;
- The Management of Token ID Rollover (STS402-1, and IEC 62055-41 Ed 3);
- The new DKGA04 (HMAC) and EA11 (MISTY1) algorithms in STS202-3 (and IEC 62055-41 Ed 3); and
- The extended Vending Key attributes for risk management that are supported by the new Key Management Centre.
- Currency token support (STS202-1) is often referred to as an STS6 feature, although it does not depend on STS600-4-2 and is in fact available in the STS/Legacy firmware.

Prism also identifies its new Security Module firmware – which supports these standards – as "STS6".

3.2 Market & use cases

Adoption of the standards collectively referred to as "STS6" is mandatory:

- All STS tokens contain a "Token ID" field that protects against forgery and misuse. This field reaches its maximum value in November 2024. Vending Systems that are not compliant with STS402-1 at that time will no longer be able to issue tokens, and meters will no longer be able to accept tokens.
- STSA members were informed about the consequences of and timelines for migration to STS6 in the document STS1800-3 "TID Rollover Checklist and Timeline".

- Several years before the 2024 deadline, Prism will stop supplying Security Modules with STS/Legacy firmware, and the STSA Key Management Centre will stop issuing legacy Key Load Files. From that time on only STS6 Security Modules (and vending systems compliant with STS600-4-2 and the other STS6 standards, integrated with an SM having STS6 firmware) can get keys from the KMC.

3.2.1 Deployment

- The STSA Key Management Centre (developed by Prism) supports STS6 (as of May 2016).
- Prism's Security Modules (with STS6 firmware) support STS6 (as of May 2016).
- Vending Systems should adopt STS6 by Q4 2018.
- Supply Group (vending key) owners may adopt DKGA04 once it is supported by the Utility's vending system. DKGA04 is backwards-compatible with legacy EA07 and brings immediate security benefits to an STS deployment.
- Meters may adopt the EA11 algorithm once it is supported by the Utility's vending system(s). EA11 meters must be deployed into a DKGA04 Supply Group.

3.3 Key benefits

Adapted from "AUW 2016 Presentation – Trevor Davel"

- Future-proof security: proactive update so that next generation of STS products meet or exceed the security standards of Smart Grid.
  - Elliptic Curve (ECC P-384) and AES-192 cryptography for key management.
  - DKGA04 uses HMAC-SHA256 to derive meter keys (for EA07 or EA11) from a 160-bit Vending Key.
  - EA11 allows meters to use a 128-bit MISTY1 key.
- Simpler logistics: improves supply chain security by ensuring that the Security Module cannot be modified or substituted; SM ships directly from manufacturer to customer (no longer via KMC).
- Enables TID rollover per [STS COP 402-1].
- Enables risk management: the Security Module enforces key usage rules on behalf of the key owner, allowing the key owner to control the magnitude of a risk event.
  - The key owner can choose which SMs are authorized to use the Vending Key, set resource and currency limits (per SM) to control the maximum financial risk, and a key expiry date (per SM) to control the duration of risk.
  - Together these allow the key owner to quantify the maximum financial risk attributes to the Security Module, and provide a loss control mechanism that shuts down ghost vending.
- STS6 firmware supports Currency token per [STS202-1]. With currency tokens the tariff tables are located in the meter rather than the Vending System; this is a good fit for Smart Meters, and enables Time-Of-Use billing.

4 PrismToken

4.1 What is it?

PrismToken is a new concept in the STS environment. It is not a new category of product, but rather is *part of a Vending System*. Specifically it is the part that has the ability to issue STS tokens and manage STS vending keys.

- PrismToken combines an STS6 Security Module, vending key store, and the STS "POS Application Process" into a single product that is readily integrated into a Vending System. PrismToken has a web-based User Interface to manage STS vending keys, and a Thrift network service that the Vending System calls to issue STS tokens.
- To issue an STS token for a meter, third-party software integrating with PrismToken only needs to know the meter's configuration (SGC, KRN, TI, EA, TCT) in order to issue an STS token. PrismToken handles all other details of the STS environment.
- PrismToken provides a low-effort quick-turnaround approach to bring the benefits of STS6 into a vending system.
- PrismToken is not a full vending system; rather it is the component of a vending system that issues STS tokens:
    - PrismToken is focused on implementing just the STS standards.
    - In particular PrismToken *does not* provide any of the following: point of sale, database of meters, customer accounts or debt collection, tariff support, business rules (other than the STS POS Application Process rules), transaction database, reporting, reconciliation and settlement.

4.2 Value proposition

PrismToken is a Commercial-Off-The-Shelf (COTS) product that can be used by Vending Systems that need to support STS. It provides turnkey STS token issue that is fully STS compliant and is easily integrated into a Vending System using a simple high-level API. PrismToken is kept up-to-date as the STS standards evolve.

4.3 Key benefits

PrismToken provides the following key benefits:

- STSA Certified token creation, complying with: [IEC 62055-41 Ed 3], [STS600-4-2], [STS531-1-0-02], [STS531-1-0-04], [STS202-1], [STS202-2], [STS202-3], [STS202-5], [STS202-6], and [STS402-1].
- Secured by Certified[1] Security Module.
- Fast and easy integration via a Thrift API.
- Supports [STS600-4-2] key management including integration with the new Key Management Centre.
- Risk Control features like vend value limits and passive key revocation are provided by Prism SM extended metadata that controls key use (see [PR-D2-0970]). The metadata is configured at the KMC (see [PR-D2-1001]), allowing the Utility to control risk and protect revenue irrespective of who is operating the SM.

[1] HSM with FIPS or PCI-HSM certification; STS functionality certified by STSA

- Base Date and TID Rollover support [STS402-1].
- Supports next-generation security including HMAC DKGA and MISTY1 EA [STS202-3].

4.4 Core functionality

The core functionality of PrismToken – which developers would otherwise need to implement in their Vending System – includes the following:

- Communicates with the SM using the drivers and low-level API (STS6).
    - SM supports DKGA=04 and EA=11 per [STS202-3].
- Implements [STS600-4-2] key management processes using the SM, so there is no need to handle STS key management operations in the Vending System:
    - Provides a User Interface to key management features.
    - Generates VKLOADREQ that can be e-mailed to the KMC.
    - Parses an STS6 Enhanced Key Load File received from the KMC, loads the Vending Keys contained therein, and maintains a store of Vending Key metadata and corresponding SM key register.
    - Provides Key Expiry warnings required by [STS 202-6].
- Thrift API to issue Credit (class=0), MeterTest (class=1), Management (class=2), and Key Change tokens.
    - Communication over TCP/IPv4 with Transport Layer Security (TLS).
    - Implements TokenID conversion with respect to the Vending Key's Base Date (BDT) per [IEC 62055-41] and [STS402-1].
    - Maintains a store of TokenIDs issued per meter to prevent TokenID duplication (POSApplicationProcess equivalent of Token Cancellation).
    - Provides TransferAmount encoding for unit and currency tokens per [IEC 62055-41], [STS202-1], and [STS202-5]. Currency encoding is validated against the STSA VSM.
    - Supports 2-digit and 4-digit Manufacturer Code in meter PAN per [IEC 62055-41] and [STS202-2].
    - Supports Rollover Key Change tokens for BaseDate change (and associated TID rollover).
    - Supports 2-token (EA=07), 3-token (EA=07), and 4-token (EA=11) key change sets per [IEC 62055-41] and [STS202-3].
    - The API is specified using the Thrift Interface Definition Language (IDL), from which client software can be automatically generated.
- Supports Prism instruction certificates (to convey SM manufacturer instructions to the SM) (see [PR-D2-0970] and [PR-D2-0828]).
- Provides a User Interface to miscellaneous SM configuration options and diagnostics.
- Handles the token generation portion of an STS transaction in a manner compatible with [SANS 1524-6-10].
- STSA certified Point Of Sale (Entity Type A), tested against [STS531-1-0-02] and [STS531-1-0-04].

In addition PrismToken maintains all this functionality in the face of ongoing evolution of the IEC specification, STSA standards, Security Module, and Key Management Centre.

4.4.1 What PrismToken doesn't do

- Provide for meter registration, MSNO[1] vending, or a meter configuration database.
- Implement [SANS 1524-6-10] (XMLVend) business rules (such a Grace Purchases, or resolving discrepancies between a meter's magstripe card and the meter configuration database).
- Conversion of currency amounts to STS transfer units, by means of a Tariff mechanism.
- A database (or log) of vending transactions or tokens issued.
- Any form of "service point" or "point of connection" management.
- Any form of customer management, accounting, or debt collection.

This functionality must be provided by the Vending System.

4.5 Relationship to SM API

The Security Module (SM) is the component of an STS system that secures the Vending Keys (VKs) and allows them to be used to construct STS tokens. While the SM will only construct well-formed tokens (per IEC 62055-41), it has limited ability to enforce STS operational rules or ensure that the token is fit for purpose.

Using an SM is necessary for building an STS vending system that complies with the IEC standard and STSA rules, but is not sufficient.

PrismToken provides high level capabilities that result in a fully compliant subsystem for issuing STS tokens; these capabilities include:

- Management of vending keys and association with Supply Group Codes (SGCs).
- TokenId management to prevent the issue of duplicate tokens to a meter, and to restrict issue of Special Reserved tokens.
- Conversion of token fields (such as TransferAmount and TokenId) to and from STS representation, with correct rounding.

To issue an STS token for a meter, third-party software integrating with PrismToken need only know the meter's configuration; PrismToken handles all other details of the STS environment.

4.6 Relationship to XMLVend

XMLVend is an XML-based protocol for Point-Of-Sale (POS) devices to communicate with an STS vending server. XMLVend is standardised in [SANS 1524-6-10].

XMLVend assumes that the server integrates with POS and technical support systems, and supports functions such as payment and customer care; all of which are out of scope for PrismToken. Token issue is a subset of the back-office functionality provided by a vending server, and as such the token issuing subsystem (PrismToken) cannot accept XMLVend requests.

[1] Meter Serial Number Only (MSNO) vending looks up the meter's configuration in a database given on the PAN or DRN (serial number).

It would be typical for PrismToken to be a component of a vending system that supports XMLVend. PrismToken is designed to handle the issue of STS tokens within certain XMLVend transactions, in the manner prescribed by [SANS 1524-6-10] and other Eskom documents.

5 Amendment History

Version	Description	Person	Date
1.0	First draft to outline value proposition.	TrevorD	2016-08-15
1.1	Restructured the document and integrated PrismToken details from PR-D2-1009, PR-D2-1010 (internal document), and various other internal documents. Updated PrismToken details to include latest supported STS standards.	TrevorD	2018-10-15
1.2	Editorial updates.	TrevorD	2018-10-26
1.3	Editorial updates.	TrevorD	2018-12-03
1.4	Updated section 1 to clarify the use of Vending Keys and their relationship to the Supply Group Code.	TrevorD	2018-12-12