African Utility Week | Clean Power Africa

The largest global meeting place from African Utilities

17 - 19 May 2016
Cape Town, South Africa

STS600-4-2 Key Management System

- Trevor Davel
- Technical Team Leader
- Prism (a Zazoo Limited business unit)
- South Africa

PRISM

zazoo

www.african-utility-week.com

OVERVIEW

- STS600-4-2 Companion Specification:

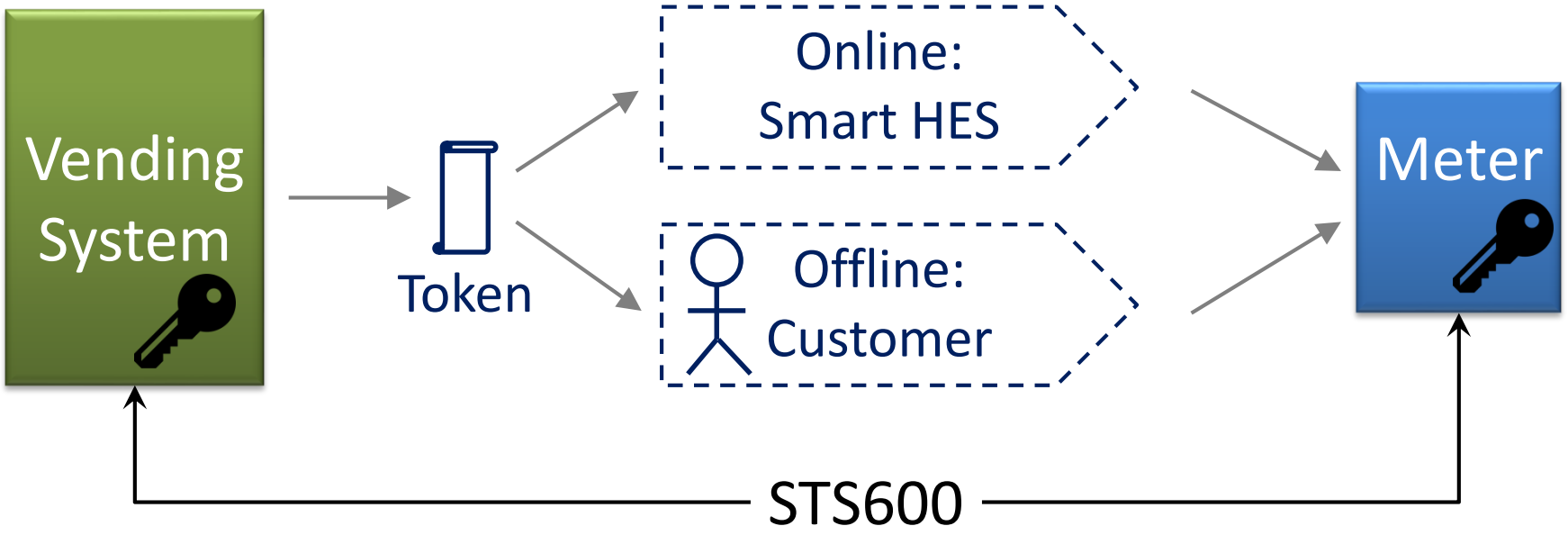
  KEY MANAGEMENT

- New Key Management Centre
- Changes & benefits
  - Risk reduction strategy to stop ghost vending
- Impact
- Questions

STS ASSOCIATION

STS (IEC 62055-41)

- Vending System creates a token (instruction)
- Token updates credit register in a meter



SECURITY MODULE (SM)

- Only SM can handle Vending Keys [IEC 62055-41]
  - Vending System must use SM to create tokens
- Security Module:
  - Keys can be used (subject to rules) *but not copied*
  - Small attack surface; Tamper response
  - Certified to FIPS (US Govt) or PCI-HSM (banking)
- Account for Security Module = Account for Keys
  - Keys protect your revenue stream

STS KEY MANAGEMENT

- Vending System must use SM to create tokens
- Meter must contain a key supplied by a Key Management Centre (KMC) [IEC 62055-41]
- Meter Manufacturers must use SM to install initial key (DITK) in meter [IEC 62055-41]
- Key management:

Get Vending Keys
from central repository (KMC)
to Security Module

STS600-4-2

- Standardises interface between KMC and SM:
  - Security Module Initialisation (once off in manufacture)
  - Vending Key Load (periodically in operation)
- State of the art security techniques
  - Standards-based (ISO, NIST, ECRYPT II)
  - Matches or exceeds Smart Grid
  - Independent security review
- *Much* more secure

DETAIL OF SECURITY TECHNIQUES

- Security target: 128 bits
- Key hierarchy: stronger security at higher levels

Key	Size (Strength)	Algorithm
Meter Key	128 bit (128)	EA11: MISTY1
Vending Key	160-bit (160)	DKGA04: KDF-HMAC-SHA256
Key Load File KEK	192-bit (192)	AES (CCM mode)
Key Agreement Key	384-bit (192)	ECDHE C(1e,2s), NIST P-384

BENEFIT: FUTURE-PROOFING

- Future-proof security
  - Proactive update for next generation of STS products

SECURITY MODULE INITIALISATION

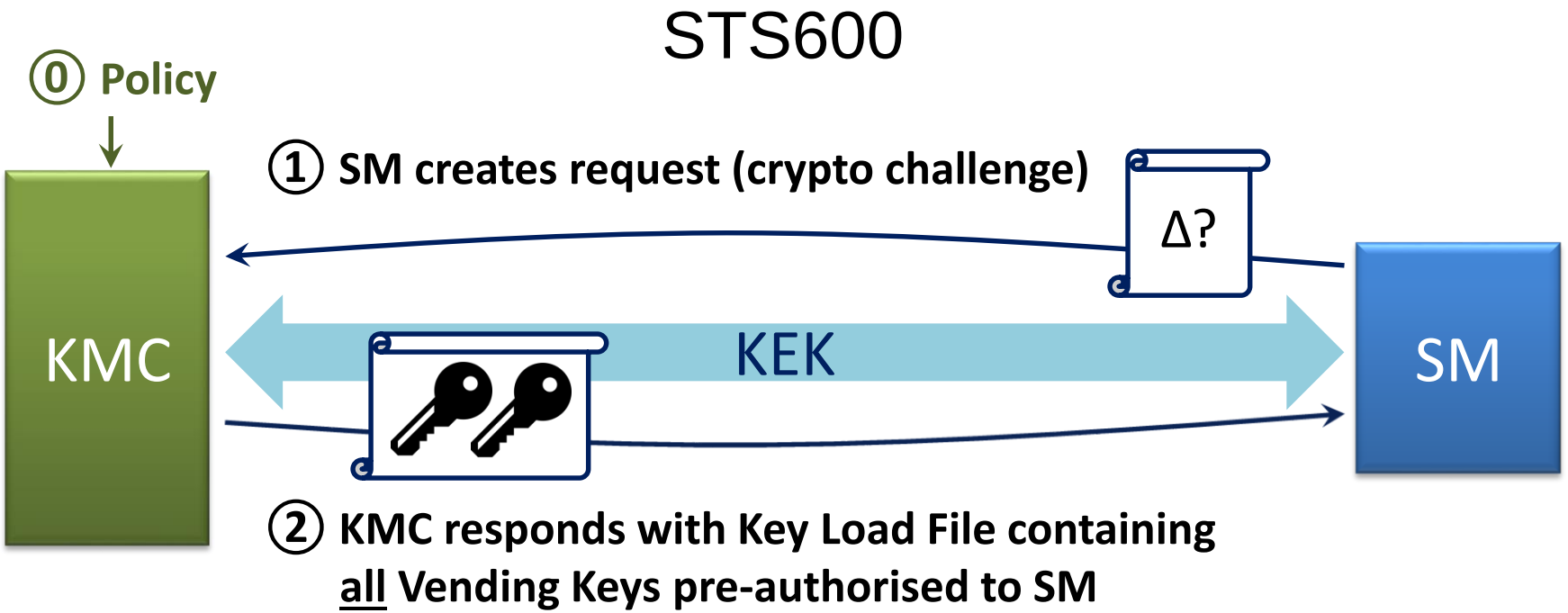
- Purpose: create a secure link between the SM and the KMC
- Legacy: send SM to KMC to get MEK & KEK
- STS600: SM initialised by manufacturer
- SM generates two related keys: secret, public.
  - Secret key known to SM exclusively
  - Public key sent to KMC
- No customer interaction with KMC

BENEFIT: SUPPLY CHAIN SECURITY

- Future-proof security
- Simpler logistics; Supply chain security
  - SM initialised by manufacturer; no shipping to KMC
  - Secret key: SM cannot be modified or substituted
  - Design informed by Payment Card Industry

VENDING KEY LOAD

- Purpose: convey keys & data from KMC to SM
- Legacy: request specific keys on co-signed form



ENHANCED KEY LOAD FILE

- *Much* more secure
  - 192-bit AES encryption with integrity protection
- Extensible meta-data per key
- Meta-data is bound to key
  - Protected & inseparable
  - Enables true benefits of STS600 & KMC

BENEFIT: ENABLES TID ROLLOVER

- Future-proof security
- Simpler logistics; Supply chain security
- Enables TID Rollover
  - Previous AUW: STS COP 402-1 (2011) defines Base Date ratchet; waiting on secure key management to roll out.
  - Timeline & impacts: STS1800-3 on STSA website
  - Upgrade Vending System to support new KLF & SM
  - Issue Rollover Key Change Tokens by 2024

RISK MANAGEMENT

- Biggest financial risk: theft of Security Module
  - SGC (vending key) owner loses account of keys
  - "Ghost vending"
- Aim: control the magnitude of a risk event
- Approach: Policy-based control
  - Key owner expresses Key Use Policy at KMC
  - Security Module enforces key usage rules on behalf of the key owner
  - Obey the vending key owner, not the SM operator

KEY USE POLICY

1. SMs allowed to use this key
2. Policy Expiry Date
   - Passive key revocation
   - Duration of risk
3. Unit Limit & Currency Limit
   - Maximum financial risk
4. Refresh Period
   - Force periodic check in case policy changes
   - Check (refresh) using Vending Key Load interface

Account for which SMs have your keys

Limits per SM allow you to understand the risk of having your keys in that SM

EXAMPLE: KEY USE POLICY

- Policy for one identified Security Module:
  - Policy expires 31 Dec 2016, refresh period 60 days
  - Unit Limit 1,000,000 kWh
- On 1 Jan 2017: vending stops
- After SM issues 1M kWh: vending stops
- SM unaccounted for?
  - Revoke policy at KMC, vending stops within 60 days
- SM accounted for, continue vending?
  - Get a fresh Key Load File from the KMC

BENEFIT: RISK MANAGEMENT

- Future-proof security
- Simpler logistics; Supply chain security
- Enables TID Rollover
- Risk management
  - Key use policy enforced by Security Module puts key owner in control
  - Quantify maximum financial risk attributable to SM
  - Loss control mechanism shut downs ghost vending

NEW KMC

- Replace ageing infrastructure
  - Improve Disaster Recovery
  - Upgrade Security Modules
- Transitional support for legacy SMs & KLFs
  - Key migration from Eskom KMC
- Security & continuity of service

BENEFIT: MULTIPLE KMCS

- Future-proof security
- Simpler logistics; Supply chain security
- Enables TID Rollover
- Risk management
- Multiple KMCs
  - SM can get keys from one or more KMCs
  - Deploy your own KMC instead of using third party services

IMPACT

- Won’t affect deployed STS meters
- New KMC & SM ready to go
- Impact primarily on Vending Systems
  - Support new Key Load File & SM
  - Issue Rollover Key Change tokens by 2024
- KMC interaction:
  - Key owners express Key Use Policy to KMC
  - Vending Systems **must** get fresh KLF periodically
  - KLF contains all keys authorised to SM

BENEFITS (SUMMARY)

- Future-proof security
- Simpler logistics; Supply chain security
- Enhanced Key Load File
- Enables TID Rollover
- Risk management
  - Loss control stops ghost vending
- Multiple KMCs

CONCLUDING REMARK

- STS complements Smart Grid:
  - 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

QUESTIONS

- *STS Association*
  - *www.sts.org.za*
  - *STS600-4-2*
  - *STS1800-3*

STS600-4-2 Key Management System

- Trevor Davel
- Technical Team Leader
- Prism (a Zazoo Limited business unit)
- South Africa

STS ASSOCIATION