W3C Web Payments IG

External Topics

2014-10-27

David Ezell - NACS

Goals

- Review the charter and goals of the IG
- Do high-level investigation of comparable work both inside and outside W3C
- Choose relevant concrete deliverables that are in scope of the charter
- Identify task forces that should be launched and that may lead to new WG or new requirements to existing WG. (the list below will be revisited, expanded or reduced during the meeting)
  - Wallet
  - Secure Authentication
  - NFC

ISO 8583

- Comparison to ISO 20022
  - Based in Business Processes - yes
  - Reusable Components – not really
  - Syntax – bitmaps, not XML (no schemas)
  - Older, but smaller

ISO 8583 – Business Processes

Position	Meaning	Usage
x1xx	Authorization Message	Determine if funds are available, get an approval but do not post to account for reconciliation, Dual Message System (DMS), awaits file exchange for posting to account
x2xx	Financial Messages	Determine if funds are available, get an approval and post directly to the account, Single Message System (SMS), no file exchange after this
x3xx	File Actions Message	Used for hot-card, TMS and other exchanges
x4xx	Reversal and Chargeback Messages	Reversal (x4x0 or x4x1):Reverses the action of a previous authorization. Chargeback (x4x2 or x4x3): Charges back a previously cleared financial message.
x5xx	Reconciliation Message	Transmits settlement information message
x6xx	Administrative Message	Transmits administrative advice. Often used for failure messages (e.g. message reject or failure to apply)
x7xx	Fee Collection Messages	
x8xx	Network Management Message	Used for secure key exchange, logon, echo test and other network functions
x9xx	Reserved by ISO	

ISO 12812

- "Mobile Financial Services"
- Status
  - Committee Draft (CD) published April 2014
  - Reviewed by ANSI (US)
  - Recommendation to ISO TC68/SC7 was sent by WG10 on October 15, 2014, to proceed with an International Standard (IS)
- Structure
  - Parts 1-5 address various mobile payment scenarios
  - Introduces the concept of "Mobile Financial Service Provider"
  - MFSPs are now covered in the requirements
    - banks, mobile network operators, trusted service managers, non-bank hosts
- Intent
  - Reuse ISO20022 and ISO8583 as the basis for describing exchanges for Mobile Payment
  - Financial institutions or retail merchants will be in a position to write RFPs based on the ISO standards so that any successful vendor must demonstrate how its products or services conform to the standard.
- Issues
  - JTC1 (through TC68) intended for the committees to harmonize ISO8583 (US) with ISO20022. This harmonization has not happened as intended.

ISO 12812 – cont.

- US (ANSI) Comments on the CD
    - Add requirements so the standard reads more like a standard than advice.
    - Identify the role of Mobile Financial Service Providers.
    - Add ACH requirements to the SEPA and EMV requirements, effectively addressing ISO8583 requirements in addition to ISO200222.
    - Add language that indicates there are no new financial services required to address Mobile use cases.
    - Change references to "secure element" or "trusted execution environment" to be more general, i.e. "secure environment" in order to address "cloud" processing of sensitive data.
    - Deconstruct section 6 (Mobile Banking) and move relevant sections to other areas of the document.

ISO 12812 – cont.

- Part 1 – General Framework
    - Terms, national laws and regulations
- Part 2 – Security and Data Protection for Mobile Financial Services
    - ISO 9564 (differentiate between an "individual device" and a merchant device
- Part 3 – Financial Application Management
    - Application life-cycle control, e.g. commissioning and decommissioning applications
    - Ability for the consumer to "opt-out" at will
    - MFS provider must provide a consumer with all Terms of Service, including rights and obligations related application lifecycle management
- Part 4 – Mobile Payments to Persons
    - Flows for SEPA, EMV, ACH and wallets
    - Assure freedom of choice with regard to device and network
- Part 5 – Mobile Payments to Businesses
    - Credit, debit, direct debit, stored value, wallets
    - Online and offline payments – definition of user identification methods (UVM)

ISO 12812 – cont.

- Part 2 Focus – Security Requirements (new since the CD)
  1. An MFS provider SHALL provide mutual authentication and follow specific requirements.
  2. An MFS provider SHALL take commercially reasonable steps to protect sensitive data from unauthorized disclosure.
  3. An MFS provider SHALL take commercially reasonable steps to protect sensitive data from unauthorized modification or substitution.
  4. An MFS provider SHALL treat authentication credential (e.g., passwords, PINs) and account numbers (e.g. PAN) as sensitive data.
  5. An MFS provider SHALL ensure that the mobile device and/or MFS be capable of logging specific events.

ISO 12812 – cont.

- Part 3 Focus – Consumer Rights
    - Maintenance of applications (embedded or downloaded) to enable consumers to gain access to updates, new features, and security patches;
    - A mechanism for applications to communicate with the software level of the Mobile Device (and/or security environment in the mobile device) in order to verify any maintenance of existing applications;
    - A process for an MFS provider to decommission an application, including when a business decision has been made not to provide the application after a certain date;
    - Articulation of rights or options a consumer has if he/she wants to retain an application purchased from a MFS provider after decommissioning, as well as discussion of any security vulnerabilities associated with retaining an application that is no longer supported by a MFS provider;
    - A process to enable the consumer to remove an application at his/her option; and
    - Management of transitive responsibilities from related service providers (components).

ISO 9564

- Part 1 - Basic principles and requirements for online PIN handling in ATM and POS systems

- Part 2 - Approved algorithms for PIN encipherment

- Part 3 - Requirements for offline PIN handling in ATM and POS systems

- Part 4 - Guidelines for PIN handling in open networks

  - The **cardholder** contacts the **merchant** using a network access device that communicates via an open network.

  - The **merchant** communicates with its **acquirer** either via an open network or through normal merchant-to-acquirer communications.

  - The **acquirer** communicates with the **issuer** using the conventional authorization and settlement networks.

  - Focus – difference between "merchant owned" and "cardholder owned" devices.

ARTS / NRF UPOS

ARTS UnifiedPOS Devices

- Belt
- Bill Acceptor
- Bill Dispenser
- Biometrics
- Bump Bar
- Cash Changer
- Cash Drawer
- CAT
- Check Scanner
- Coin Acceptor
- Coin Dispenser
- Electronic Journal
- Electronic Value Reader/Writer
- Fiscal Printer
- Gate
- Hard Totals
- Image Scanner
- Item Dispenser
- Keylock
- Lights
- Line Display
- MICR
- Motion Sensor
- Mag Stripe Reader
- Pin Pad
- Point Card
- POS Keyboard
- POS Power
- POS Printer
- Remote Order Display
- RFID Scanner
- Scale
- Scanner
- Signature Capture
- Smart Card Reader
- Tone Indicator

ARTS / NRF UPOS – Printer Methods
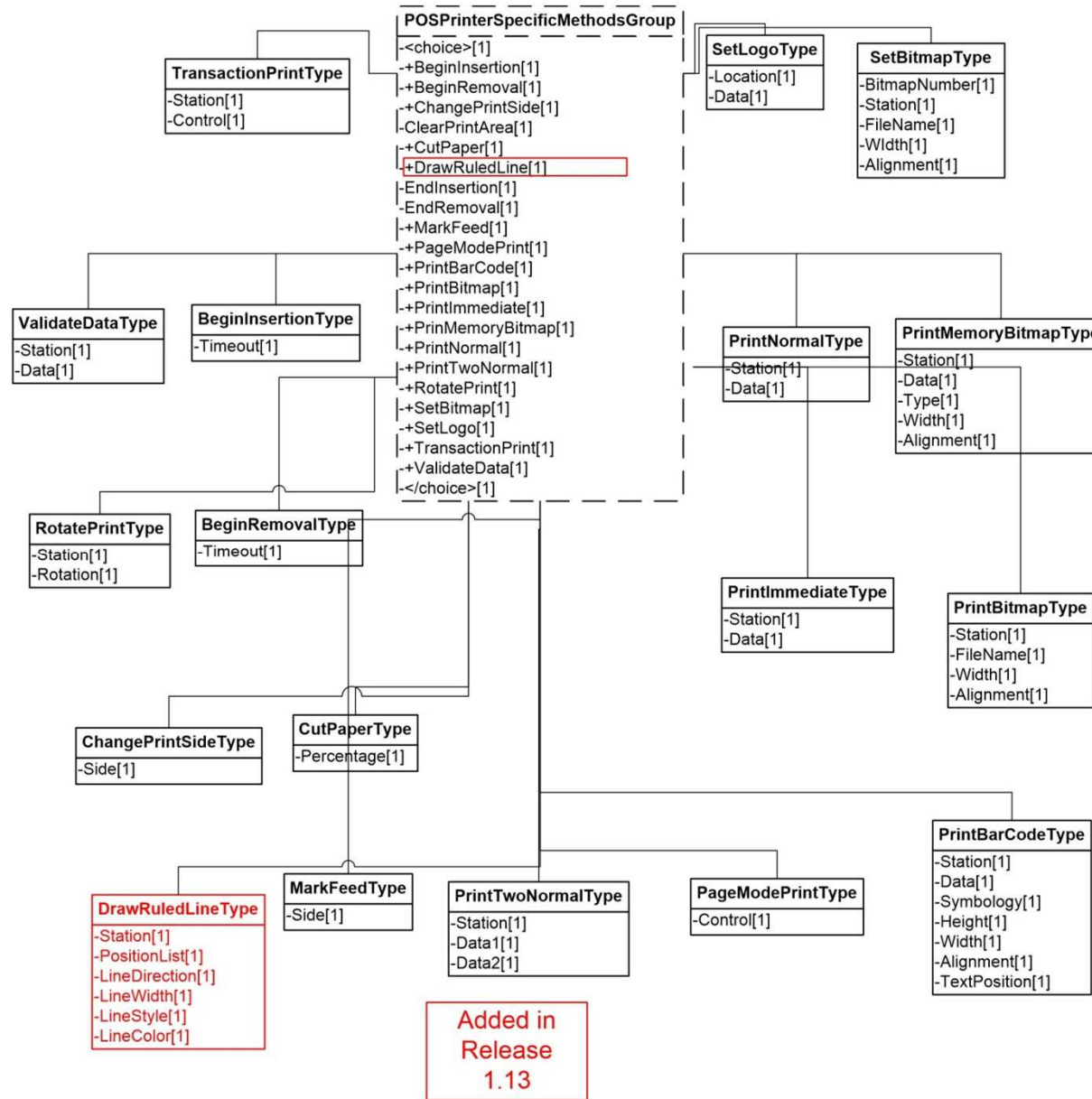
EPAS

- Electronic Payment Applications Software
- European focus
- Three specifications
  - Terminal Management
    - Configuration, troubleshooting, maintenance
  - Retailer Application
    - Touch points for application business logic
  - Acquirer Protocol
    - Back end communication

EMV Payment Tokenisation

- EMVCo "Standard"
- Ecosystem
  - Token Service Provider
  - Card Holder
  - Card Issuer
  - Merchant
  - Acquirer
  - Payment Network
  - Token Requestor (any above)

- Data Elements
  - ISO 8583
- TSP Requirements
- TSP API Guidelines
  - Might be a target?
- Payment Token Processing
- Payment Token Flows

Backup

X9

- EPAS for Dummies:
  http://viewer.zmags.com/publication/c47b8ceb#/c47b8ceb/8

- Introduction to SEPA:
  http://ec.europa.eu/internal_market/payments/sepa/faq/index_en.htm

- Introduction to ISO8583:
  http://en.wikipedia.org/wiki/ISO_8583

Templates

TITLE
Sub Title

Date

TITLE

Title

- Bullet
- Bullet
  - Sub Bullet
  - Sub Bullet
- Bullet