CMS Interfaces

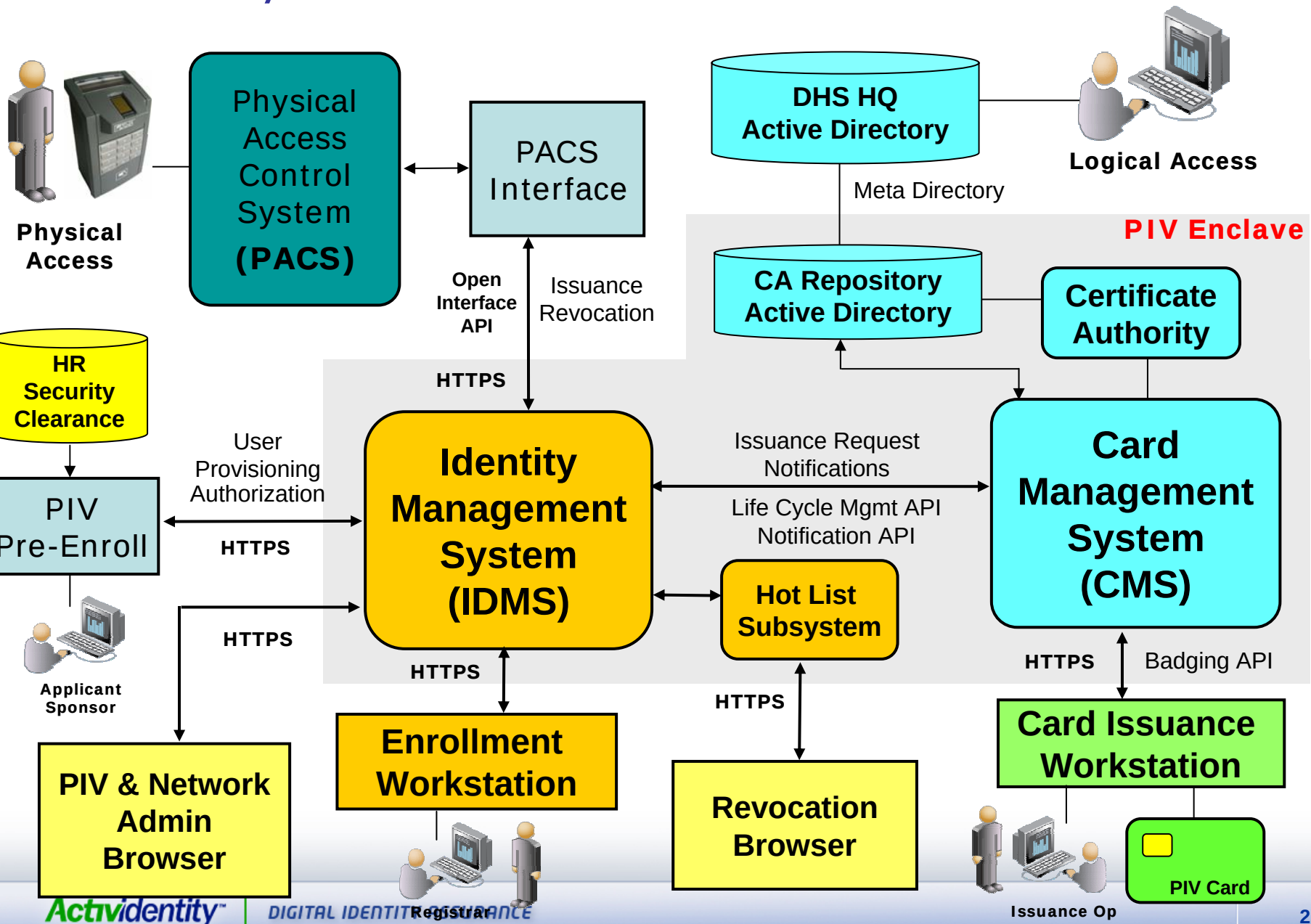
ActivIdentity

Dom Fedronic - CTO Office - v1.0 - 04-15-06

ActivIdentity™

DIGITAL IDENTITY ASSURANCE

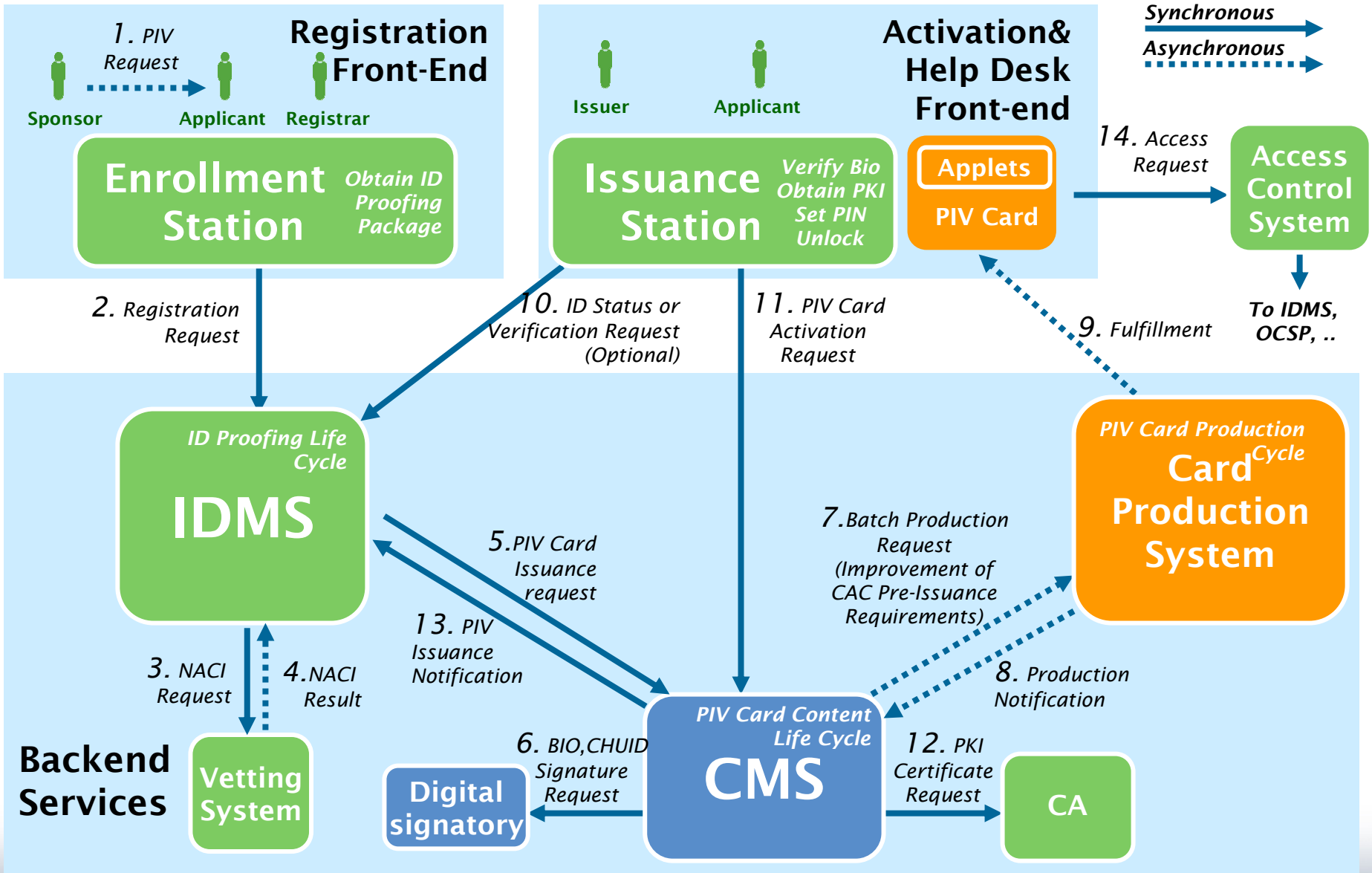
DHS PIV System Architecture



Interfaces of the CMS

- Interface with the IDMS:
  - Card Issuance Request
  - Card status notification
- Interface with Credential Providers
  - CAs
  - Digital signatories
- Interface with the Card Production Facilities (Service Bureaus)
  - Based on an extension/update of PIR4.2

PIV general architecture



Interfaces of with the IDMS

- The Card Issuance Request
  - XML
  - Implemented at DHS with LMCO IDMS
  - Supports PIV
  - Extensible
  - Secure: XML_DSIG, XML_ENC /W3C
  - Transaction Oriented
  - Transport insured by the Card Life Cycle Mgt API (card/credential management API)
- The Card Status Notification
  - Leverage CIR transaction data
  - Returns issuance status
  - Plugins. Implemented at DHS
- Published 2005 (Life Cycle Management, Badging).

Interfaces of with Credential Providers

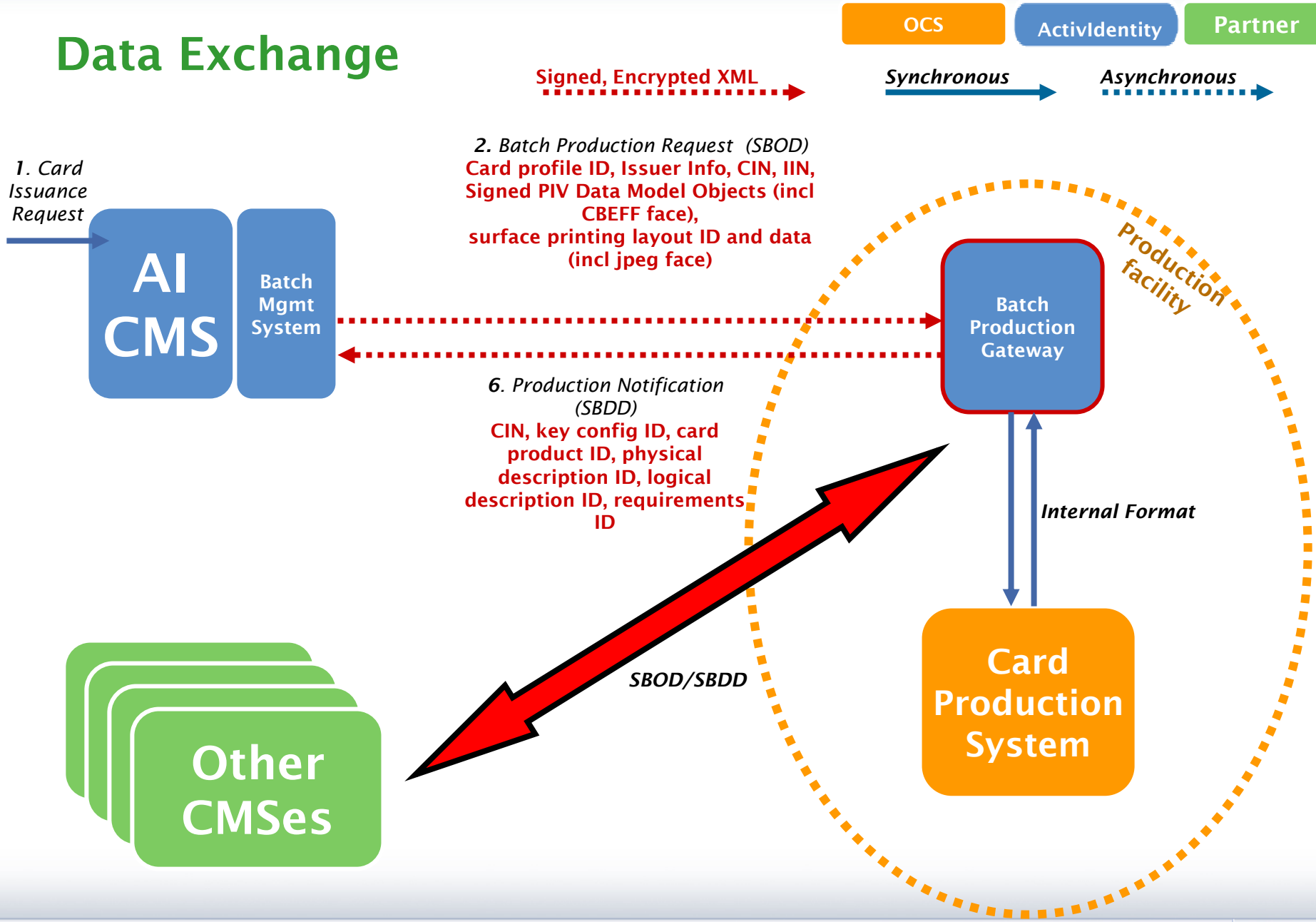
- SPI
- Full Abstract Credential Life Cycle Management
- Supports CA
- Supports Digital Signatory services
- Supports Biometrics sub systems Identification and verification.

Interfaces with Card Production Facilities

Requirement:

- Open
- XML based
- Extensible
- Cover the requirements for PIV Card Production
- Secured (proof of origin and integrity, and confidentiality) .
- Should leverage an existing standard in a backward compatible manner: Should be backward compatible with PIR.

Data Exchange



Leverage Pre-Issuance Requirements specifications

- PIR fulfills need for interoperable format between Issuers and Shared Production Service Providers
- Each production facility can support simultaneously multiple issuers (service provider model).
- Each Issuer can support simultaneously multiple production facilities (Current PIR 4.2 / DoD CAC production model)
- New Issuers can be supported with limited impact on the production system
- New Production facilities can be supported with limited impact on the Issuer
- Needs Personalization data in SBOD
  - Alignment with FIPS201 Data Model

PIR, a Proven Data Interchange Specification

- PIR has been used to produce several millions of CACs:
  - Multiple manufacturing sites
  - 1000s issuance sites
  - Multiple card types
  - Multiple card profiles (CACv1, CACv2)
  - Centralized Issuance or face-to-face
  - Now version 4.2
- Production contract between Card Issuer and Card Production Facility.
- Self Contained.
- Batch Oriented.
- Defines two XML message format for transmission of data specific to a batch.

Standard – Secure - Open

- Standard
  - XML schema, xml-dsig, xml-enc, W3C
  - Backward-compatible with Pre-Issuance requirements
  - Design to support 800-73 Data model encoding & FIPS201 layout
- Security
  - Proof of origin, confidentiality, integrity to transport sensitive data in various contexts, possibly offline and asynchronous.
- Open
  - 800-73 Data model extensions
  - New Applications

SBOD/SBDD

- SBOD/SBDD
  - Service Bureau Order Descriptor / Delivery Descriptor
- Purpose
  - Complete Card Production Protocol
    - Encompasses all card production directives in a single message
  - Support bulk card production of personalized PIV cards (SBOD)
    - Provides product configuration, personalization data, delivery site and contact to production facility or Service Bureau.
  - Support notification of card production for further activation and post-issuance (SBDD)
    - Returns status and identifiers of produced card/credentials

Call for Action

- Already started to engaged with the PIR editing community.
- Already engaged with Global Platform
- Engage with Security Industry Association
- Early draft.

For Additional Information

Contact:

Dom Fedronic
CTO
ActivIdentity
dfedronic@actividentity.com