

Dedicated Security Components (DSC)



Introducing The DSC PP iTC

May 19, 2017 | ICMC 2017 | Arlington VA

Shawn Geddis

Chair, DSC iTC
geddis@apple.com



Shawn Pinet

Deputy Chair, DSC iTC
shawn.pinet@gemalto.com

Dedicated Security Components

How the iTC came to be

- 2014 –CCRA updated to cPP and EAL2
- 2015 – ICCCC Windsor: HSM TC + NIAP Mobile
- 2016 – CCUF Reading: ESR Drafted
- 2017 – CCUF Amsterdam: Survey of PPs, Use Cases, Vendor Diagrams, Services, Assets, Threats Defined
- 2017/2018 – Version 1?

DSC iTC

Community Working Together — 77

Schemes

- DE - Germany
- IN - India
- JP - Japan
- NL - Netherlands
- SE - Sweden
- UK - United Kingdom
- US - United States

Vendors

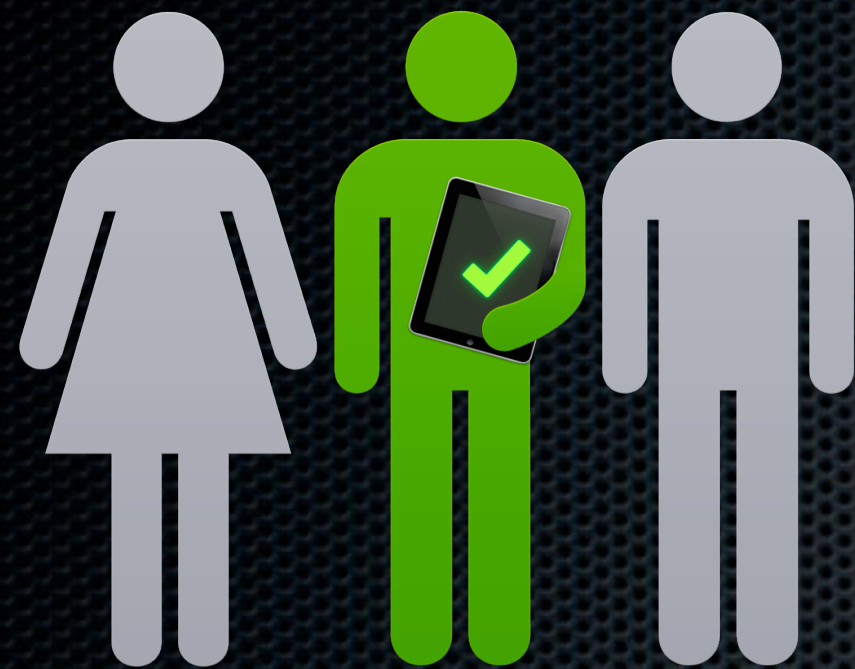
- Phones
- Tablets
- Wearables
- Smart Cards
- Semiconductors
- HSMs

Schemes — 7 (25 people)

Vendors — 12 (19 people)

Labs — 12 (19 people)

SMEs — 14 people



Dedicated Security Components

Where are we in the process?

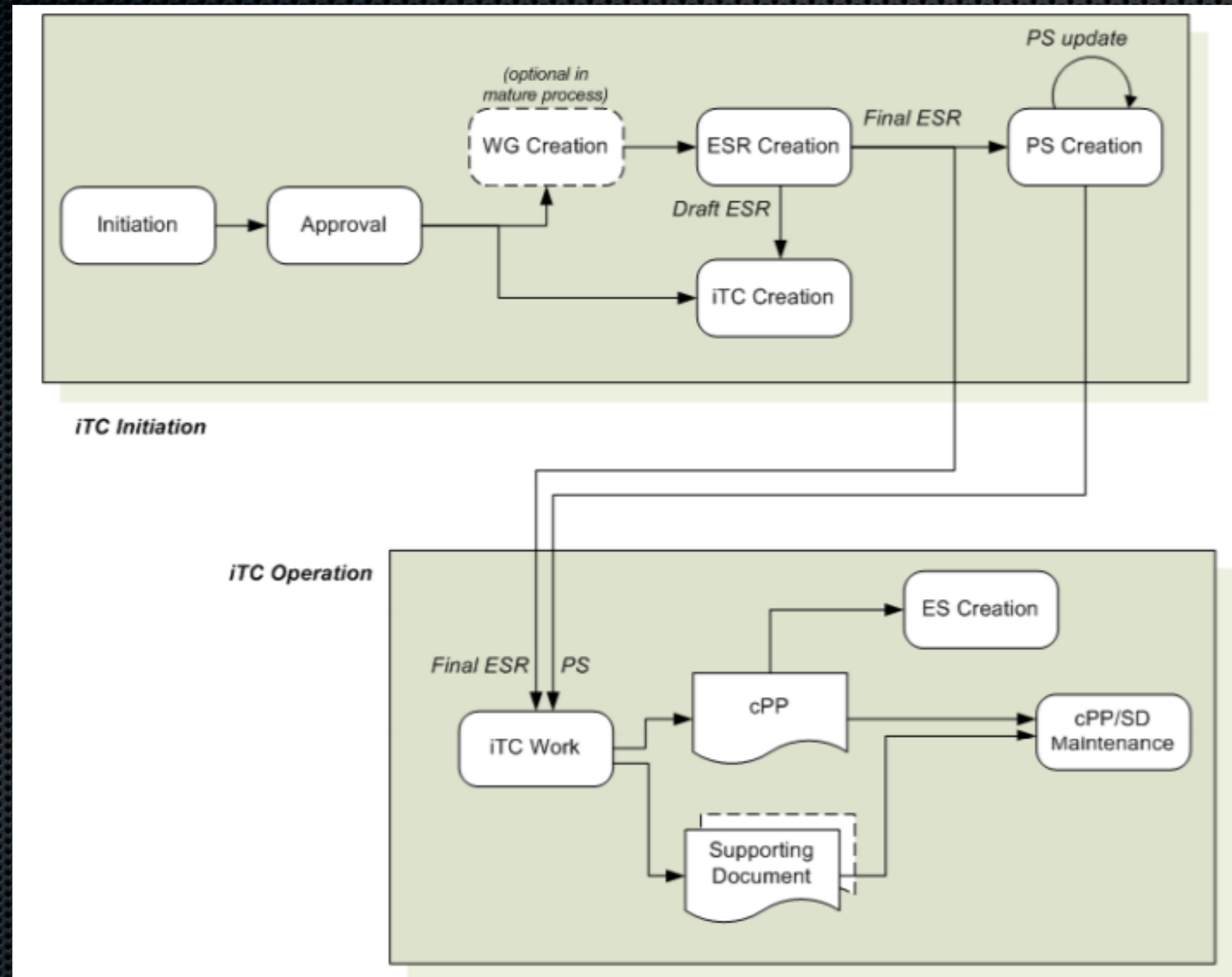


Figure 1: High-Level View of iTC Initiation & Operation⁴

Dedicated Security Components — DSCs

What are the use cases?

- User Managed Credentials (Passwords)
- Mutually Managed Credentials (P2P identities)
- Enterprise Managed Credentials (Device Authentication, High-value data)
- Multi-Party Credentials (Payments, Digital Signature)

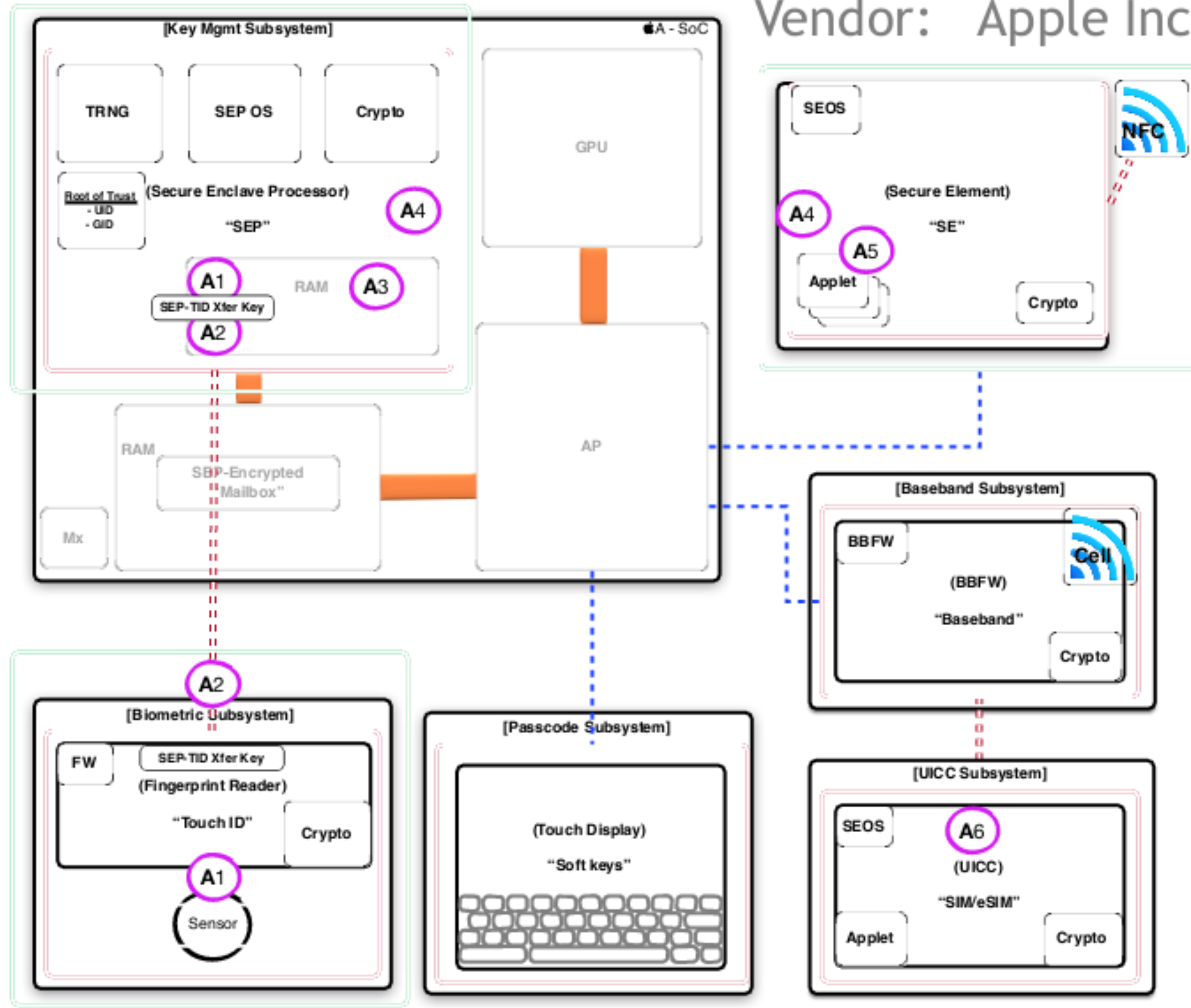
Credentials are the ultimate security data elements to be protected.
Threats and objectives will map back to the use cases

Dedicated Security Components — DSC

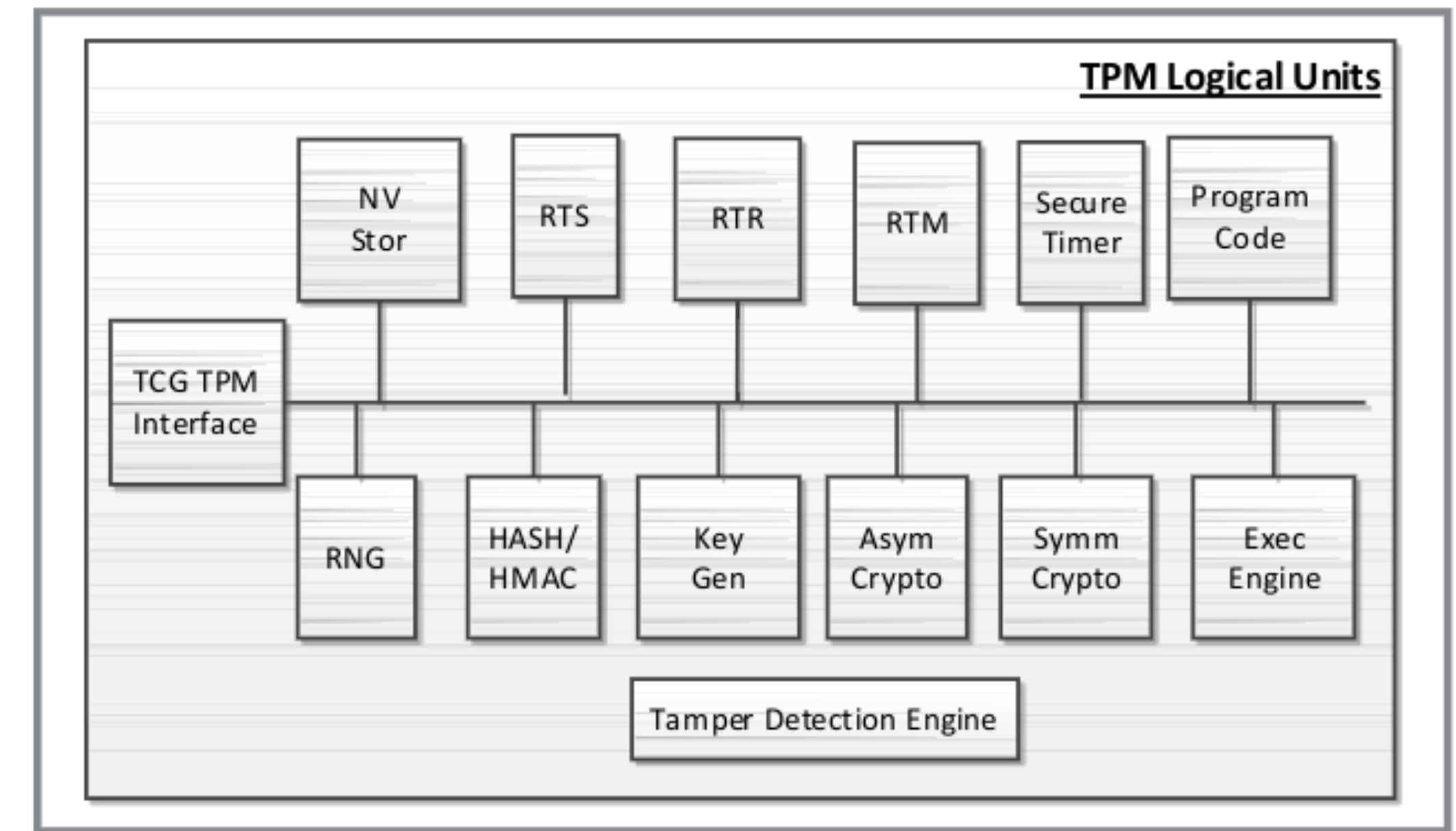
Vendor Reference Diagrams

Apple DSC - Dedicated Security Component

Vendor: Apple Inc.



Vendor: Intel



Dedicated Security Components

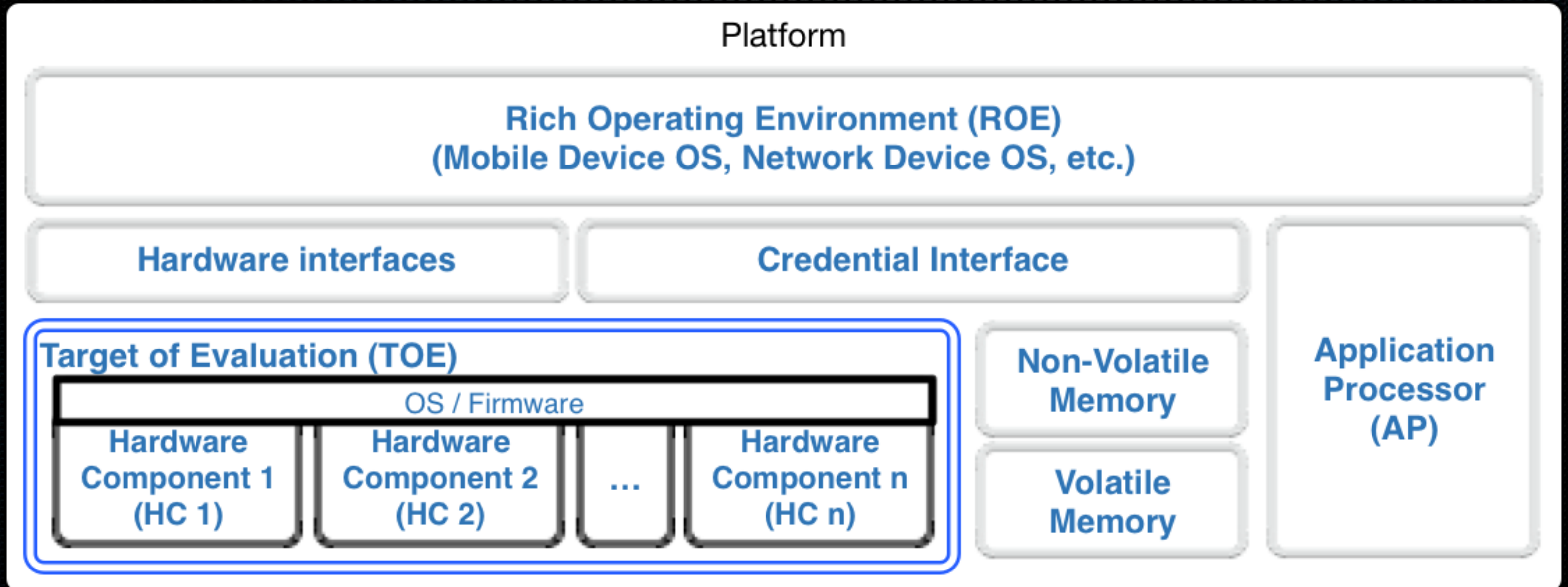
DSC defined

“A composition of one or more discrete hardware components dedicated to managing the protection and use of credentials.”

Credentials are the ultimate security data elements to be protected.

Dedicated Security Components — DSC

The TOE – a collection of one or more hardware components

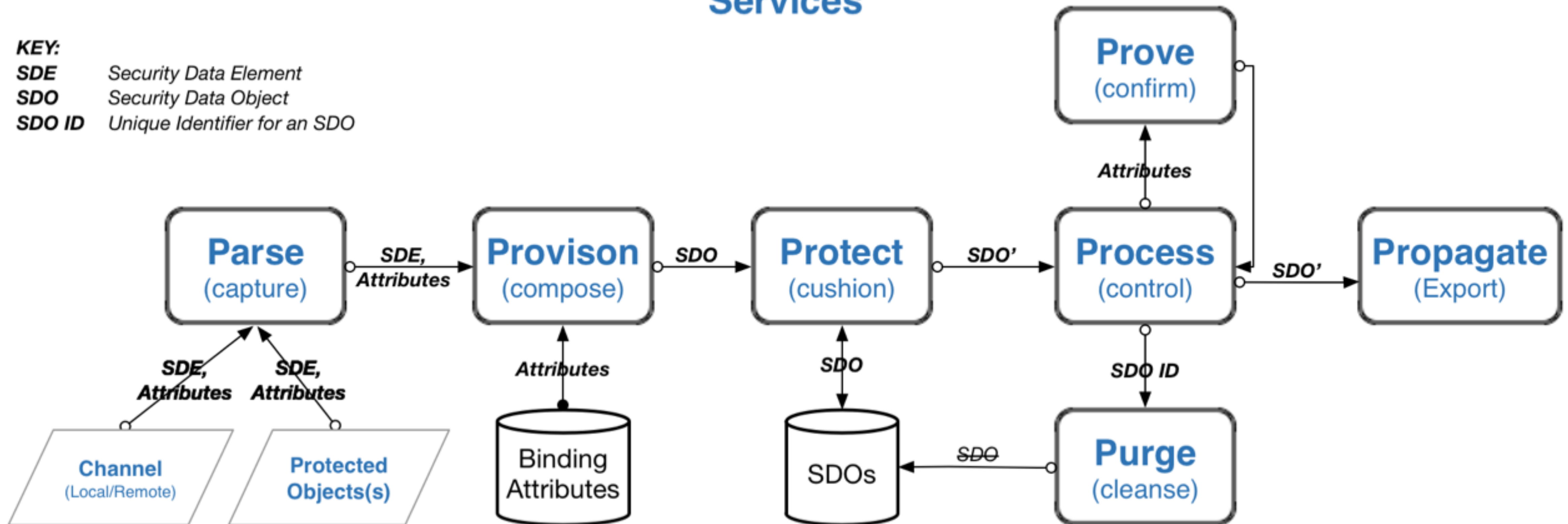


Dedicated Security Components — DSC

The 7 Common Services

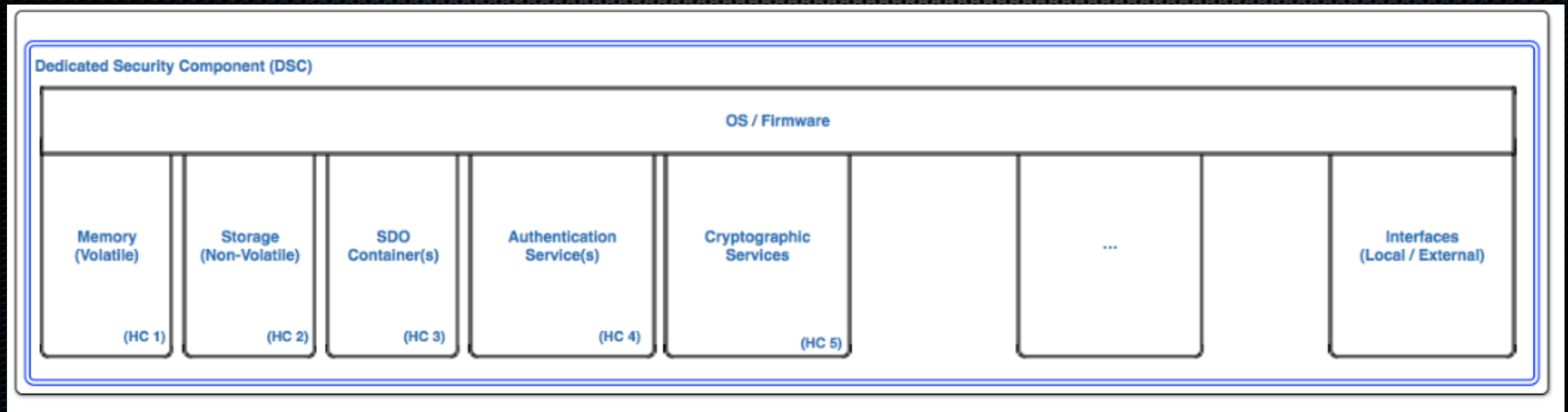
Services

KEY:
SDE Security Data Element
SDO Security Data Object
SDO ID Unique Identifier for an SDO



Dedicated Security Components — DSC

TOE – Components and functionality



Dedicated Security Components — DSC

Binding data objects

Security Data Object (SDO)

Binding Data (BD)

**Security Data
Element 1
(SDE 1)**

**Security Data
Element 2
(SDE 2)**

...

**Security Data
Element n
(SDE n)**

DSC cPP

Driving global requirements

Bridging (some of the) IT Security Certification chasm

- **Not a replacement, but rather additive to existing PPs**
 - *DSC PP will be a modular approach with other PPs*
- **Speed of Certification**
 - *Goal is to complete in ~90 days leveraging automation*
 - *Maximum re-use of pre-existing tests*
- DSC PP will be a modular approach with other PPs – **Aligning with existing PPs** (*i.e.. MD PP, FDE, ND PP, ...*)
- **Already certified components** — *leverage existing certifications activities where possible to reduce the time to completion to 90d*
- **Mutual Recognition (cPP)** — FIPS is not mutually recognized ☹

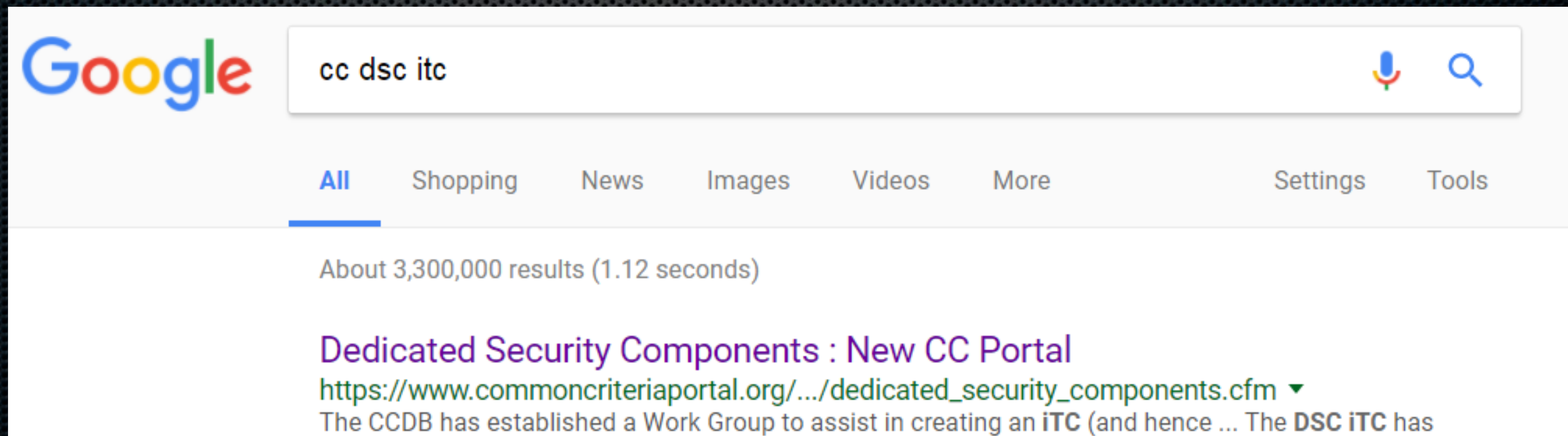
DSC cPP

How do I join?

ITC-DSC@niap-ccevs.org.

<https://ccusersforum.onlyoffice.com> “Dedicated Security Components iTC”

https://www.commoncriteriaportal.org/communities/dedicated_security_components.cfm



Dedicated Security Components (DSC)



Shawn Geddis

Chair, DSC iTC
geddis@apple.com



Shawn Pinet

Deputy Chair, DSC iTC
shawn.pinet@gemalto.com