Common Criteria Recognition Arrangement
Development Board

CCDB DSC cPP WG

Title: **Dedicated Security Components (DSC) Essential Security Requirements**
Maintained by: **CCDB Work Group for Dedicated Security Components**
Version: **1.2**
Date of issue: **2016-May-24**
Supersedes: **1.0**

Status

Developers of Smart Devices have developed an Essential Security Requirements (ESR) document for the development of a Dedicated Security Components (DSC) collaborative Protection Profile. Even though there is currently no cPP for DSCs, there is a related protection profile "Security IC Platform Protection Profile with Augmentation Packages" registered and certified by BSI [BSI-CC-PP-0084-2014]. That PP should be interpreted by the iTC as contributing to the development of a separate DSC cPP. The related PP focused squarely on the discrete IC component manufacturer rather than the device manufacturer as well as lacked the existence as a cPP for global recognition.

It is believed that a Dedicated Security Components (DSC) cPP should be developed within an iTC with a scope of dedicated security hardware component domains and their inter-domain communications for each of the four use cases identified in this ESR.

Background and Purpose

Smart devices have become so pervasive in our daily lives that their use as an authoritative identity and for daily transactions has come to be expected. The mobility of a device containing highly sensitive credentials and information brings with it concerns for securing those credentials during their lifecycle on the device. Smart device security technology is rapidly advancing with competing approaches to solving these security and privacy challenges. However, accelerated technology advances have left a void in the formal definition and affirmation of acceptable hardware-based implementations.

Users of all kinds are increasingly reliant on smart devices (phones, tablets, wearables, etc.) for access to sensitive resources, credentials, payments, and corporate and personally identifiable information. The need for mobility with access to these resources at anytime, from anywhere has crippled organizations using traditional means of credential protections and authenticated access. Users have come to expect their smart devices can and should enable faster and smoother access to ever expanding capabilities.

Those responsible for securing the information on those devices are increasingly challenged beyond available resources and lack reference-able certifications of appropriately implemented technology. All involved need assurance that information remains safe and private for an ever expanding use of their devices. With increased functionality comes increased use, increased attack surface and variations of smart device access to sensitive information. Credentials of all types have varying lifecycle duration, origination and threats associated with their daily use - possible exposure to unauthorized individuals or systems.

Developers of Smart Devices have incorporated technologies to increase functionality while also providing needed protection. Developers of smart device protection mechanisms have shifted from simple software controls to full-on dedicated hardware with most implementing a composite of dedicated components for providing the needed protection. Variations in developer approaches are not only expected, but paramount in the advancement of technology and enablement of new functionality.

Developers of Smart Devices have begun pursuing and achieving validation of their platforms with respect to the operating systems and services. However, with rapid advancements in technology, a void has formed in the formal definition and affirmation of certified security hardware-based implementations within the boundary of the devices.

Dedicated Security Components (DSCs) would be formally defined as a composition of discrete hardware component domains and the inter-domain communication dedicated to the provisioning, protection, and use of credentials for the identified use cases with their corresponding security requirements.

This ESR describes four identified Use Cases and their high-level security requirements. It provides a set of requirements for each use case targeted at mitigating well defined and described threats. In addition to stating what properties the composite DSCs will exhibit, the ESR also expresses functionality that vendors could optionally consider for use cases defined in future versions of the cPP. Furthermore, the ESR identifies aspects that are outside the desired scope so as to limit the final set of security functional requirements specified in the cPP, as well as the evaluation activities performed during the course of an evaluation.

The logic behind scoping the components' capabilities to be specified in the cPP is to ensure that objective and repeatable evaluation activities can be captured in the cPP while still delivering a cPP in a timely manner. Additionally, we aim to ensure the baseline security functionality prescribed is not beyond current commercial technology and is achievable by multiple developers and multiple products.

Today's smart devices have discrete hardware components with each providing a well scoped security function. The protection of intercommunication and exchange of sensitive security parameters between these components is as critical as within the hardware boundary of each component.

Dedicated Credential Stores "HW-Isolated Credential Store"
Some Dedicated Security Component domains will protect security sensitive data (ie. credentials, keys, tokens) using embedded components that provide the following services in hardware isolation:

- **Parse**
  The DSC ingests pre-provisioned keys, credential, tokens, etc. from trusted components external to its boundary across a secure channel or in a secure manner.

- **Provision**
  The DSC can generate cryptographically sound keys, credentials, tokens, etc. entirely within its own boundary.

- **Protect**
  All security data elements stored inside the component are protected inside the boundary. If bound to the hardware, they are also inaccessible in raw form outside the boundary by other non-DSCs such as application or baseband processor(s) on the platform.

- **Process**
  The DSC processes the sensitive credential(s) on behalf of component(s), external to the DSC, using keys and/or controls protected inside the DSC, but only after a cryptographically authenticated parameter is provided via a trusted path.

- **Purge**
  The DSC cryptographically purges each security data element when it is no longer needed to protect against unauthorized recovery.

Authenticated Authorization - Credential Unlock "Secure Authentication"
Dedicated Security Components will utilize security sensitive data within its boundary with authenticated authorization. DSCs for authentication in smart devices are largely focused on, but not limited to a subset of biometric modalities (e.g. fingerprint / facial) as well as the ever present entry of a known passcode. The iTC should consider including the following methods.

- **Biometrics**
  Fingerprint recognition is by far the most common form of biometric modality found on today's smart devices. Advancements in speed and accuracy in recognition have made it the most common form of biometrics found. Successful fingerprint matching unlocks authorized access for a DSC to begin using provisioned and protected credentials. The state of biometrics on these devices today has prevented its direct use as an encryption key, but has allowed its use as an appropriate authenticated access control mechanism.

- **Passcodes**
  The use of user-entered passcodes still remains as a time-tested approach to authentication on devices. Appropriately derived passcodes can also be used to derive Key Encryption keys (KEKs) and frequently are involved in a key hierarchy for the protection of data-at-rest.

- **Token**
  The use of a provisioned, trusted and hardware protected credential uniquely identifying one device to another. This could be in various forms such as a sufficiently generated key or token.

Use Cases

Use Cases defined here are designed to be building blocks with each successive use case building on the capabilities and security functional requirements of the previous use cases(s), unless otherwise noted. Suggested real world examples for each use case is also provided.

[Use Case #1] User Managed Credentials (Single Information Owner)

These credentials are selected and maintained by a user to prove their identity and access personal resources locally or through remote internet services. The user might be required to meet basic requirements such as the cryptographic strength of the credential (ie. length and complexity of a password), but the selection and continued use of the service is completely up to the user. The user is in full control of the lifecycle of their credentials and wants them to be protected from unauthorized use.

Personal Identification for Communication or Data Access

Most users utilize some form of internet communication such as email, social networking, publicly accessible internet services, etc. A product with DSCs could ensure the user is who they claim to be by leveraging the continual hardware protection of a credential trusted by the service.

[Use Case #2] Mutually Managed Credentials (Dual Information Owners)

These dynamic and typically ephemeral credentials are negotiated between two parties (or trusted systems on behalf of the parties) for the purpose of exchanging data privately between two endpoints. There is no third-party — independent authority — involved in the lifecycle of these credentials. The user/device is in control of the lifecycle of their credentials and wants them to be protected from unauthorized use.

Peer-to-Peer Identification and Privacy

Privacy is founded on the ability to assure that the content being shared remains within the boundary of those authorized to access it. Peer-to-Peer communication has a long history of problems in how to ensure you are communicating with whom you intended as well as keeping content to only the intended recipient(s). A product with DSCs could ensure the recipient(s) are who they claim to be by leveraging the hardware protection of a mutually trusted credential. Upon successful validation of the recipients' identity, the product could use the cryptographic services of the DSC to isolate the exchange between peers and ensure only the intended recipient(s) can access the content.

[Use Case #3] Enterprise Managed Credentials (Enterprise Information Owner)

These tightly managed credentials require compliance with policies that exceed a user managed case, because of the risks to highly sensitive information if the credential was compromised. The enterprise will require additional assurance that the credential remains safe and protected while on the device especially when the enterprise may not have full management control of the device. The enterprise is in full control of the lifecycle of the credential.

User / Device Authentication to Enterprise Managed Resources

A product with DSCs will enable authenticated access to data or services from an authorized user and/or device. A product with a hardware-secured Mobile ID facilitates the use of a mobile device as a secure and reliable form of authentication for authorized access to highly sensitive local and/or remote data and services.

High-value Data Protection

Protection of high-value data requires additional assurance that there is little, if any, chance of an attacker ultimately gaining access to the encryption keys used to keep data safe and away from unauthorized entities. A product with a DSC, protecting the corresponding Data Encryption Keys (DEKs) or Key Encryption Keys (KEKs) which in turn protect the DEKs inside of a DSC, increases the protection of sensitive and high-value data against brute force attack both online and offline. Increasingly sensitive data can then be accessed, processed and stored on the smart device.

[Use Case #4] Multi-party Credentials (Multiple Information Owners)

These tightly protected and managed credentials require compliance with policies from multiple parties that exceed an enterprise managed case, because of the increased risk to all parties involved if the credential was compromised. All parties will require additional assurance that the credential remains safe and protected while on the device especially when all parties other than the user have no management control of the device or platform. Ultimately, the credential issuing authority controls the validity and acceptance of the credential. Multi-party credentials, as the name implies, involves multiple parties to handle the credential in some form during a given transaction. Each party must be assured and have the ability to verify the validity of the credential prior to performing their part of the transaction.

Mobile Commerce

A product with DSCs could provide secure storage and protected use of tokens for financial transactions between trusted and authorized users, devices, merchants and financial institutions. These DSCs would provide safe use of the tokens inside the protected hardware boundary. The use of certified hardware-isolated credential stores on smart devices and only unlocking their use with authenticated authorization provides confidence that the transaction was indeed authorized by the approved 'device holder'.

Resources to be protected

Dedicated Security Components (DSCs) are a composition of one or more discrete hardware components dedicated to managing the protection and use of credentials. Credentials themselves are the ultimate data elements to be protected. There are possibly many inter-related and layered resources used in the protection of the credentials for each use case which, if any one of these layered resources were individually compromised, could lead to compromised credentials.

- **Credentials generated and/or stored within the boundary of the embedded component.**
  First and foremost, the protection of security data elements (keys, credentials, tokens, etc.) with their lifecycle defined inside the boundary of the DSCs, hardware-based, must remain inside with no external access to the raw data. Data elements defined as hardware-backed, are those provisioned externally, securely transmitted to the DSC must have the remaining lifecycle taking place inside the boundary of the DSC with no external access to the raw data.

- **Data elements used to access the credentials stored on the smart devices**
  The DSC used for storage of credentials must require a trusted and authenticated authorization element, such as authorization factors, keys, and key material, be presented and validated prior to the use or release of a DSC protected data element.

- **Trusted system software, or firmware, that runs within the embedded component.**
  Software/firmware that is executed as part of the operational environment of the DSC shall be protected from unauthorized modifications. Updates to the software/firmware shall be cryptographically validated by the DSC to ensure the origin of the update as well as the integrity of the update itself.

- **Configuration data stored within the boundary of the embedded component.**
  When a DSC relies on configuration data for tasks such as validation of data element exchange with an external component, or the mapping of internal data elements with externally provided references (i.e. Key References), the DSC must protect those data elements from being modified or accessed directly by any unauthorized external component.

Attacker access

- An attacker gains logical access to the DSC through a programmatic weakness in a trusted component or a secure channel.
- An attacker with privileged access can intercept and arbitrarily modify or drop data within existing traffic flows to and from the DSC.
- An attacker can intercept and modify software/firmware updates destined for the DSC.
- An attacker gains access to the DSC's physical interface and can attempt to physically and logically modify sensitive information or trusted software executed within the DSC's boundary.
- An attacker gains physical access to the smart device with enough time to attempt exhaustive physical and logical attack on the DSC.

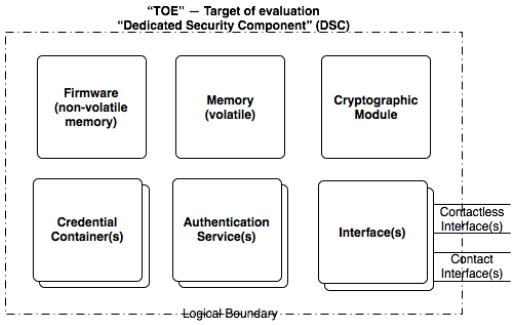
Attacker Resources

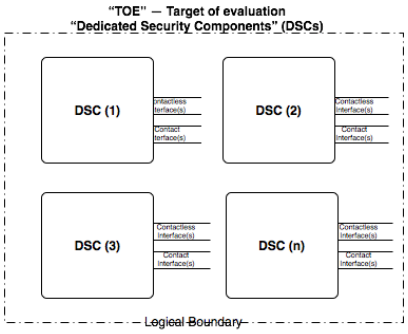
- Arbitrary amount of time to examine and attack the embedded component's physical and logical interfaces both online and offline.
- Commercially and/or publicly available software/knowledge/equipment. The tools available to attackers are expected to be sophisticated enough such that strong cryptography will need to be used to protect the data, since direct examination of the physical interface may be possible.

Boundary of Component

Dedicated Security Components (DSCs) are a composition of one or more discrete hardware component domains and inter-domain communications dedicated to managing the protection and use of credentials.

- The TSS must specify the physical security boundary of the TSF.
- The hardware/firmware/software supplied by a composition of component domains as part of a product installation form the logical boundary for DSCs.
- Channels between composite DSC domains are considered inside the logical boundary.
- Interfaces between DSCs and external components are considered inside the logical boundary.





Essential Security Requirements

The ESR expects products to employ approved cryptographic algorithms to protect credentials from unauthorized disclosures. The ESR expects the product to invoke cryptographic functionality in the Operational Environment (OE) within a composition of one or more hardware-based DSC. For each use case, the resulting cPP is expected to be divided into two sections; those requirements that a defined DSC must meet and those requirements the underlying platform must meet. Since the ESR covers multiple implementations involving hardware, firmware and software, certain requirements and Assurance Activities may only apply to certain use cases.

As noted in the Use Cases section above, each Use Case defined here is designed to be a building block on top of each previous use case — building on the security functional requirements of the previous use cases(s), unless otherwise noted. The following requirements for each Use Case should be considered by the iTC and altered or moved between Use Cases or augmented as deemed appropriate by the iTC.

Incrementally increasing requirements to be met by the composition of DSCs are the following:

[Use Case #1] User Managed Credentials
(*The user is in full control of the lifecycle of their credentials***)**

Integrity

- The DSCs shall protect keys, key material, and authentication credentials from unauthorized disclosure and alteration.
- The DSCs shall provide self-tests to ensure the functions it implements are operating as designed.
- The DSC shall have internal security features to make the device more resilient to security breaches.

Cryptography

- The DSCs shall be able to derive KEKs from authorization factors, appropriately conditioning any authorization factors so that they can be used as a KEK or combined to form a KEK(s).
- The DSCs shall zeroize/secure erase all authorization factors, plaintext secrets, private cryptographic keys and cryptographic security parameters when no longer required.
- The DSCs shall wrap any DEK(s) with one or more KEK(s) using approved key-wrapping algorithms.
- The DSCs shall rely on trusted entropy source(s).

Authentication

- The DSCs shall provide a lock-out mechanism for failed authentication attempts.
    - A lock-out mechanism would prevent continued use of any DSC security data element without administrative remediation or a delay before subsequent authentication attempts are allowed.
    - A lock-out mechanism would provide mitigation against tampering by an unauthorized user or process.

Authorization

- A user must be authorized by the DSCs before utilizing any security data element within the DSC.
    - Minimum strength (entropy of authorization factor) for authorizing the use of a security data element contained within the DSC.
    - The entropy of the authorization factor shall not be weakened by choices of algorithms or any conditioning that is used in the key derivation process.

- The DSC shall determine that the authorization factors are valid prior to using protected security data elements, while ensuring that this process does not expose or reduce the effective strength of any key or key material.
- The authorization rights of the user are determined by the DSC.

Administration

- The DSCs shall provide a cryptographic means to validate the source of updates to their firmware.

[Use Case #2] Mutually Managed Credentials

(The user/device is in control of the lifecycle of their credentials)

Integrity

- The DSCs shall provide self-tests to ensure additional functions are operating as designed.
- The DSCs shall provide software/firmware integrity.

Cryptography

- The DSCs shall use approved key-agreement algorithms for exchange of security data elements between endpoints.

Authentication

-

Authorization

-

Administration

-

[Use Case #3] Enterprise Managed Credentials

(The enterprise is in full control of the lifecycle of the credential)

Integrity

- The DSCs shall provide self-tests to ensure additional functions are operating as designed.
- The security data elements protected in the DSC shall not be recoverable without a brute force attack.
- Side Channel Attack mitigation such as to defend against Differential Power Analysis (DPA) or fault injection.

Cryptography

- The DSCs shall be able to manage the lifecycle of security data elements (ie. credentials, keys, tokens) completely within their logical boundary.
- The DSCs shall rely on trusted entropy source(s).
- The DSCs shall use approved DRBG(s) within their boundary.

Authentication

-

Authorization

-

Administration

- Remote administration functions shall use strong cryptography to protect all communication paths.
- The DSCs shall be able to be subdivided into one or more "domains" which may be managed independently, providing isolation between "domains" such that information in one "domain" may not be accessible in raw form by another "domain".

[Use Case #4] Multi-party Credentials

(Each party verifies credential and authorization prior to performing their part of the transaction)

Integrity

- The DSCs shall provide self-tests to ensure additional functions are operating as designed.
- The raw security data elements protected in the DSC shall not be recoverable.
- The DSC shall be resilient to side-channel attacks.

Cryptography

-

Authentication

-

Authorization

-

Administration

-

Assumptions

- When authorization factors, such as keys, credentials, and tokens, are provisioned from outside of the component, it is assumed that the strength and entropy is commensurate with the DSC key strength.
- Well-behaved authorized users cannot leverage services that have privileged access to use protected credentials within a DSC.
- Well-behaved authorized users do not use privileged tools to modify the DSC or platform to be non-compliant with this protection profile.
- The Operating System or Platform relying on the DSCs has already been or is being independently certified against an existing protection profile.
- The protected credentials are for the sole use by a single user or device.

Optional Extensions

Requirements captured in this section may already be realized in some products in this technology class, but this ESR is not mandating these capabilities exist in products.

- Each component domain may have achieved independent certification against an existing Protection Profile.

Objective Requirements

Requirements specified here identify security-relevant behavior that is not expected to be realized currently in products, but capabilities that may be mandated in future versions of the resulting cPP.

- The DSCs shall be able to assign which interface(s) local / remote administration may take place.
- The DSC shall enforce two-factor authentication prior to use of protected credentials.
- The DSC shall enforce the use of a 'secure display' for visual verification prior to authorizing the of use security data elements from the DSC.
- The DSC shall verify the integrity of the communications channel and the identity of a recipient service before providing those services to an external process or component.

Outside the Scope of Evaluation

Requirements specified here identify those which are expected to be specified in other ESRs and resulting cPPs.

- Validation of any external credential provisioning system(s) used for authorization factors, such as keys, credentials, and tokens.
- Restricting the types of security data elements retained within the DSCs.
- Evaluation of local/remote administration tools used to provision or manage the security data elements deployed to the DSCs.
- End-to-end evaluation with the externally maintained systems relying on the security data elements protected within the DSCs.
- Validation of the Operating System or Platform relying on the DSCs.