[DSC] Storing and Processing Multi-party Credentials

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.

These tightly protected and managed credentials require compliance with policies from multiple parties that exceed a typical 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 platform especially when all parties other than the authorized user have no management control of the platform. Ultimately, the credential issuing authority controls the validity and acceptance of the credential. Multi-party credentials, as the name implies, involves multiple parties processing 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.

Private Key Store

A platform leveraging DSCs as a hardware-secured Private Key Store facilitates the use of secure and protected storage of asymmetric/symmetric private keys for access to data and services. These DSCs would provide safe use of the private keys inside the protected hardware boundary.

User / Device Authentication to Enterprise Managed Resources

A platform leveraging DSCs for a hardware-secured ID facilitates the use of the platform as a secure and reliable form of authentication for authorized access to highly sensitive local and/or remote data and services.

Mobile Commerce

A platform leveraging DSCs facilitates 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’.

Capabilities, Assumptions, and Threats

This document outlines the capabilities, assumptions, and threats for one use case for Dedicated Security Components (DSCs). It begins by listing the services for use case four. Then for each service, it lists the capabilities required to carry out the service. Then assumptions and threats follow. First we define a few terms.

Definitions

Assured Identification of Endpoints – Authentication of the source of security data element(s) received through a channel.

Binding – Strong, provable and predefined association of security data elements together into a security data object.

Peer-to-Peer – Either of two platforms can act as a server for the other in negotiating mutually trusted credentials for purposes of mutual authentication and privacy without the need for a central server.

Platform – The composition of hardware, firmware, operating system for the purpose of running processes which provide service(s) to an identified entity.

Protected Storage – Provides integrity and privacy protection to all retained security data elements. **Integrity-protected** locations prevent the unauthorized modification of the security data elements they contain (i.e. protect security data elements from unauthorized writes). **Privacy-protected** locations prevent the unauthorized disclosure of the security data elements they contain (i.e. protect security data elements from unauthorized reads). All protected storage will prevent the unauthorized use of any security data element (i.e. require proper authorization before allowing the use of security data element(s) within its boundary).

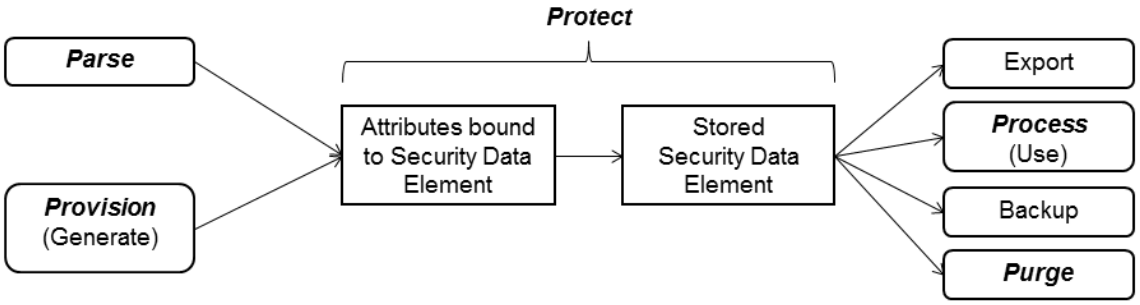
Remote Peer – The entity at the far end of a secure channel with which to negotiate the exchange and verification of keys, credentials, and tokens. A remote peer must provide a verifiable and trusted authentication token before the local peer will exchange any security data elements.

Secure Channel – An encrypted channel or one that is otherwise isolated in a way that preserves the confidentiality and integrity of the security data elements moving through it. An encrypted channel uses a random Bit generator (RBG), a key generator, and cryptographic engine to set up the secure channel and process (i.e. decrypt) the security data elements exchanged with a remote peer.

Security Data Element – An object such as a key, credential, or token used for the purpose of protection or authentication of security sensitive information.

Services

There are five core security services of a Dedicated Security Component (DSC).



Parse - The DSC ingests pre-provisioned keys, credentials, tokens from components external to its boundary across a secure channel, and stores them as secure data elements in Protected Storage. The DSC shall establish a secure channel and authenticate the identity of the far endpoint of the channel prior to parsing any secure data element.

Provision - The DSC generates cryptographically sound secure data element(s) (keys, credentials, and tokens) entirely within its own boundary or securely between two DSCs. Provisioning includes the use of mechanism(s) which create reference material and authorization requirements for authenticated access or use of the security data elements.

Protect – The DSC protects all security data element(s) within its boundary from unauthorized access. The DSC shall enforce a secure channel during the exchange with a remote peer. The security data element(s) are bound to hardware and 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 security data element(s) on behalf of its remote peer, using keys and/or controls protected inside the DSC, but only after it receives authenticated authorization(s) provided via a secure channel. It shall require a cryptographically sound engine, key generators, and RBG to fully carry out its handling of security data elements.

Purge - The DSC cryptographically purges security data element(s) when the peer-to-peer communication no longer requires it or the stored security data element is no longer needed by the platform. It will require a cryptographically sound mechanism to destroy the security data element(s) preventing further use.

Capabilities

For each of the five services, required capabilities are identified and explained. Optional capabilities may exist, but are not required in providing the service.

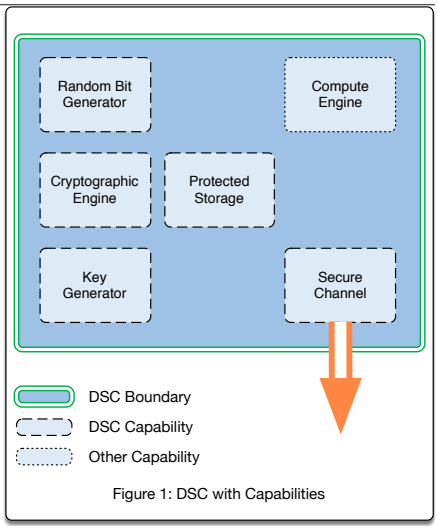


Figure 1: DSC with Capabilities

Protected Storage - All protected storage will prevent the unauthorized use of any security data element.

Secured Channel - Path through which the confidentiality and integrity of security data elements are ensured.

Assured Identification of Endpoints - Knowledge of the Source and Destination of security data element(s) passed through a channel.

Element Binding - Strong, provable and predefined association of security data elements together into a security data object.

Cryptographic Engine - uses **ISO compliant cryptography** for:

- ***Sources of Entropy*** - Use of dedicated and approved entropy source(s).
- ***Random Bit Generator (RBG)*** – Use of one or more trusted sources of entropy that are made available in the form of random bits to generate keys, seeds for key derivation functions (KDFs), nonces, authorization values, and other security data element(s).
- ***Key Generator*** – Use of approved mechanisms for generating keys for all purposes.
- ***Key Agreement -*** Use of approved key agreement algorithms to establish security data elements between remote peers.
- ***Key Exchange -*** Use of approved key exchange algorithms for exchange of security data elements between remote peers.

Roots of Trust – Use of Approved RoT for Measurement, Storage, Reporting, etc.

Secure Boot – Use of cryptographic validation of the boot process/code/path to ensure integrity of executable environment.

Software / Firmware Integrity

- ***Power-On-Self Tests (POST)*** - self-tests to ensure DSC functions are operating as designed prior to operational use.
- ***Continuous Self Tests*** - Ensure functions continue operating as designed.

Assumptions

The following is a list of assumptions about the DSC that must remain true to mitigate the identified threats.

Physical Protection – It is assumed that the device holder will ensure that an attacker has no prolonged, unsupervised physical access to the device, and therefore the cPP will not expect the device to defend against attacks such as physical modification (whether to modify device behavior or to create/access additional interfaces), side channels and fault induction attacks that rely on study and/or long-term control of the device. It is also assumed that if a device is lost or stolen then there is a method of revocation of any credentials held (or equivalent method of mitigating the impact of potential access to the credentials.

Authorized Users Authorized users follow all provided guidance regarding the safeguarding of security data element(s), especially authorization tokens such as passwords, pass-phrases, and biometrics.

Trusted Peer The peer at the other end of a secure channel is trustworthy, and will not abuse the secure channel in order to introduce malware or fraudulent security data elements into the DSC.

Threats

A threat consists of a threat agent, an asset, and an adverse action by the threat agent on the asset. In the use cases for DSC, an asset is a security data element. Threat agents put security data elements at risk if and when an adversary gains access to the device containing a DSC it can manipulate a security data element. The consequences of risks to security data elements include the loss of confidentiality of the user's content, unauthorized access to and use of the user's content, destruction of the user's content, and the ability of the adversary to impersonate the user or the user's device.

Unauthorized Access - The cPP will address the primary threat of unauthorized access to the security data elements within the DSC. If an adversary gains access to a users' security data elements, they may attempt to view, use, or destroy the user's content as well as impersonate the user or the user's device.

Security Data Element Compromise – Possession of the keys, authorization values, and other security data elements outside the context of the DSC puts the user's data, identity, and device at risk.

Weak or incomplete binding of data elements - *Threat agents may successful swap one provisioned security data element with a malicious data element of their own.*

Authorization Presentation – Threat agents may repeatedly present authorization factors, such as passwords, biometrics, etc. that protect the security data elements. Successful presentations put the user's data, identity, and device at risk.

Weak cryptography – Threat agents may cryptographically exploit poorly chosen cryptographic algorithms, ciphers or key sizes. Weak cryptography chosen by users or by TSF protection mechanisms puts the user's data, identity, and device at risk of exploitation by adversaries.

Unauthorized Update – Threat agents may force the device to update the DSC with firmware which compromises its security features. Poorly chosen update protocols, cryptographic algorithms, and keys sizes may allow adversaries to install software and/or firmware that bypasses security features and provides them with unauthorized access to security data elements.

Modular Packages

There are environments with operational requirements that exceed the protections addressed by the base security functional requirements that will be found in the DSC cPP v1.0. Additional requirements will be developed and organized into modular packages to augment the base requirements of the cPP. It is expected that more modular packages will be identified and developed beyond the two most frequently requested packages:

- ***Side Channel Attack Mitigation***
    - The DSC provides approved mechanisms to defend against Differential Power Analysis (DPA).
    - The DSC provides approved mechanisms to defend against fault injection
- ***Secure Software / Firmware Update***
    - Verify authorized origin of update prior to approving modifications
    - Update Software/Firmware