Federal Office
for Information Security

Management Whitepaper

Cryptographic Service Provider

The CSP - a concept to reduce time and costs of software certification with Common Criteria (CC)

The Cryptographic Service Provider (CSP) defines a concept to reduce security issues by encapsulating cryptographic assets like keys and other credentials from the application runtime. Security related tasks are triggered by the application, but the specific cryptographic operation is executed in an isolated environment. Sensitive assets are not transferred in an unencrypted manner to the application or other insecure environments.

Thus, the CSP is not just another cryptographic library. It is a tool which supports developers by defining a clear separation layer between functional features and security related operations. This document gives a short summary of the CSP without going into any technical details.

Concept

A CSP offers common cryptographic operations and high-level protocols to support a variety of security related use cases. Since the concept of the CSP can be applied to many technologies, the cryptographic API provided by the CSP harmonizes security solutions for different platforms (e.g. hardware chip, Cloud service). Furthermore, a CSP reduces time and costs of an application's security certification process.

Since an application does not manage sensitive assets directly, a lower certification level is adequate for the application. E.g., by using a Common Criteria (CC) EAL4+ certified CSP, a CC EAL2+ certification might be sufficient for an application that would otherwise require CC EAL4+. In the end, a complex composite certification of an application according to Common Criteria can be replaced by separate certifications of application and CSP in different but suitable assurance levels. On top, a CSP can be implemented and certified once, and then be reused by multiple applications for different use-cases.

Whitepaper CSP

Objectives

The objectives of the CSP are summarized as follows. A CSP

- offers a wide range of cryptographic operations and high-level protocols via a simplified API to support a variety of security related applications,
- provides a consistent API to harmonize security on different hardware platforms,
- allows to separate the implementation of security related features and business logic of an application to increase reliability and to prevent misuse of cryptographic assets,
- reduces time and costs for application evaluation and certification, as sensitive assets and cryptographic implementations are moved to the CSP and are not part of the application anymore.

Use cases

The concept of the CSP is a generic approach. It is suitable for many use cases with high security demand, and where cost- and time-efficient security certification is needed. Besides that, the CSP is also suitable for use cases where harmonization on different secure hardware platforms is required.

Among others, the CSP is applicable to the following use cases:

- eID on mobile devices (e.g. Smart-eID)

  The Smart-eID handles personal data like name, address and birthdate on a Smartphone and provides this data for online registration or login purposes e.g. for tax declaration, to create a bank account, or to register a SIM card. The Smart-eID uses the CSP for identification and authentication processes based on Extended Access Control (EAC) [TR-EID].

- Technical Security System for cash registers (TSE/TEE)

  The TSE is an electronic record system to sign payment transactions and to prepare them for tax declaration. The background of the TSE is to prevent tax evasion. The TSE uses the CSP to create an integrity protected audit log of the transaction, which can be exported and used for a tax audit [TR-TSE].

- Fast IDentity Online token (FIDO2)

  FIDO2 is a standard for two-factor authentication using dedicated hardware tokens. A CSP can be used to protect the private user key [FIDO2].

Common for all use cases is that they are integrating the CSP concept, on the one hand to simplify security evaluation and certification of their solution and on the other hand to offer an efficient certification process for companies implementing the particular use case. E.g., by serving simple, independent CC protection profiles for eID-Applets, TSE-applications, FIDO2-Applets, and other applications using the CSP.

Usage

The CSP offers a flexible module system to support different kind of technical architectures, e.g. a Clustering-module for high-performance CSP-solutions, or an Audit-module to expand cryptographic services. In addition, two CC protection profiles (PP) for the CSP are available to distinguish between different security demands: One for CSP-Light implementations with lower assurance levels used for environments already providing a sufficient amount of protection [PP-CSPL], and another for CSP implementations with very high security demands [PP-CSP].

This modularization within the protection profiles allows to develop many different kinds of CSP solutions. For example, CSP of the national German Smart-eID is implemented either as native JavaCard Extensions or as JavaCard Applet on Secure Elements; CSP solutions for TSE are either operated as a local hardware component, or as a HSM Cloud solution offering cryptographic online services.

Outlook

The European Commission and ENISA are currently working on new European certification schemes. For example, under European Cybersecurity Act (CSA) and Cyber Resilience Act (CRA), new schemes are developed for 5G network components (EU5G), cloud solutions (EUCS). European Digital Identity (EUDI) is currently working on an architecture framework for European Wallet solutions. The CSP as a vital component can support certification under these new schemes, taking time and cost demands of the market into account.

Roadmap of the CSP is to publish a technical specification of the CSP. Depending on feedback from current existing CSP realizations, the CSP protection profiles might be adapted to further improve the certification process.

References

[TR-CSP] Federal Office for Information Security (BSI), BSI-TR-DRAFT, v0.92, 2022
"*Technical Guideline Cryptographic Service Provider*"

[PP-CSP] Federal Office for Information Security (BSI), BSI-CC-PP-0104-2019
"*CC PP Cryptographic Service Provider*"

[PP-CSPL] Federal Office for Information Security (BSI), BSI-CC-PP-0111-2019
"*CC PP Cryptographic Service Provider Light*"

[TR-EID] Federal Office for Information Security (BSI), BSI TR-03127, v1.40, 2021, Technical Guideline
"*eID-Dokumente basierend auf Extended Access Control für Personalausweis u. Smart-eID*"

[TR-TSE] Federal Office for Information Security (BSI), BSI TR-03153, v1.01, 2018, Technical Guideline
„*Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme*"

[FIDO2] Fido Alliance, https://fidoalliance.org/