Proposed collaborative PP-Module for Continuous Multi-Factor Authentication enrolment and verification Overview

Version 1.1, November 9, 2021

Table of Contents

Chapter 1. Document Description

This is an overview of a proposed collaborative Protection Profile Module (PP-Module) used to extend a Base-PP for a computer that implements Continuous Multi-Factor Authentication (CMFA) to keep the computer in the unlocked state using a collection of CMFA inputs. Therefore, the Target of Evaluation (TOE) in this PP-Module is a computer that implements CMFA functionality. However, the terms TOE and TOE environment in this document expresses the CMFA system that implements the continuous authentication functionality, and the computer that supports the CMFA system to protect the CMFA data respectively, for clearly describing the relation and boundary between the CMFA system and computer. The CMFA enrolment and verification processes are described in the following sections.

Chapter 2. CMFA (TOE) Overview

CMFA is intended as a system for maintaining the identity of a user on a computer after the initial user authentication credentials have been successfully entered into the computer. The CMFA system works in the background to maintain a level of trust about whether the computer is still in the possession of the authenticated user. This is done by utilizing information from a variety of sources available to the computer, and then combining this input to create a score about the confidence the computer is still in the possession of that user. The score is meant to be dynamic, being updated on a periodic basis (within the limits of usability on the computer), so the level of confidence is determined with sufficient frequency to meet the security needs of the user.

CMFA as understood here is specifically defined as a system to determine this confidence (referenced as the Trust Score) using the available inputs (as determined by the device and administrator). The Trust Score is the output of the CMFA system; the actions that should happen based on that Trust Score are the responsibility of the computer. This is similar to how biometric authentication systems are generally configured; the authentication system asks the biometric subsystem to determine whether a user's identity is valid and a result is provided back to the authentication system. The main difference with CMFA is that while a biometric system is generally a yes/no result about the user's identity, the CMFA Trust Score provides a range (such as a 100 point scale) that can be used to provide a level of confidence to the computer.

In practice this means that the actions of the device are not directly determined by the CMFA system, but are implemented by the computer's authentication system based on the Trust Score and the configured threshold value(s) that correlate to actions the system must take. This division ensures that the CMFA system is able to work solely in the background with no direct user interaction (once enrolment/training has been completed). If the Trust Score has dropped below a specified threshold and the computer is locked by the authentication system, it is the authentication system that determines the user must enter new credentials (i.e. biometric/password/PIN as specified in FIA_UAU.5 in the Base-PP) to unlock the computer. The act of entering these credentials successfully would be recorded by the CMFA in the background to increase the Trust Score above that set threshold again.

2.1. CMFA Examples

There are many possible examples for CMFA usage on a computer. The key point to any of these is that the CMFA is only maintaining the Trust Score in the background, and it is up to the computer to determine what actions to take based on the value of the Trust Score.

The examples here are meant to show a range of options for the use of the CMFA output but are not meant to be exhaustive or even necessarily what is mandatory for use.

1. **Maintain Computer Unlock** - this is the simplest case, where as long as the Trust Score is above a threshold value, the computer is maintained in an unlocked state (so the user is not prompted for direct authentication credential entry)
2. **Sensitive Data Protection Lock/Computer Unlock** - this is an expansion of #1 with the additional function that if the Trust Score falls below a higher level, that SDP data (defined in the PP_MDF) would lock, while still maintaining the computer unlock for everything else. For

example a score of 85 is needed to keep SDP unlocked, and a Trust Score of 70 is needed to keep the computer unlocked. Above 85 everything is available, below 70 the whole computer is locked, but between 85 and 70, SDP is locked while everything else on the computer remains available.

3. **Time-Delay Lock -** this is a case where the Trust Score may fall below the threshold, but instead of an immediate lock action, the CMFA engine will check to see if an action happens within a period of time to raise the score back above the threshold, such as transiting between separate buildings on a campus (and losing Wi-Fi connectivity).
4. **Rich Trust Score** - this is a scenario where more than just the Trust Score is available. The additional output could include information such as whether the computer is within a specific location, or any other combination of available information (such as analysis of signal combination subsets as opposed to the entire Trust Score). Generally, this information is only provided to the computer and not the user.

2.2. TOE main security features

This is a collaborative Protection Profile Module (PP-Module) used to extend a Base-PP for a computer that implements CMFA to keep the computer in the unlocked state using a collection of CMFA inputs. Therefore, the Target of Evaluation (TOE) in this PP-Module is a computer that implements CMFA functionality. However, the terms TOE and TOE environment in this document expresses the CMFA system that implements the continuous authentication functionality, and the computer that supports the CMFA system to protect the CMFA data respectively, for clearly describing the relation and boundary between the CMFA system and computer. The CMFA enrolment and verification processes are described in the following sections.

2.2.1. CMFA Enrolment

During the enrolment process, the TOE captures characteristics to uniquely identify the user and creates a user profile. The TOE may capture samples from the biometric characteristics of the user presented to biometric sensors on the TOE (or utilize the results provided by a configured biometric sensor). The TOE may also extract other distinguishing features such as passwords, wireless signals within range of the TOE, behavioral patterns of the user, device activity, and other factors to determine the identity of the user. The user's captured data is used to create a profile that can verify the user at a later time. A user or administrator may be able to revoke or change a user's profile data (or the configuration used to create the profile data) that is captured by the TOE.

The enrolment process for CMFA may, depending on the configuration, take time to complete. Some biometric sensors may take time to learn (such as gait), or location information may be needed over time to provide the proper scoring. This period would be defined at the start of the enrolment process. Not all authentication sources will have the same period. For example, motion sensors used for gait would have a longer time than a fingerprint scanner. Each source of authentication information should have its own defined length of time it can be used for enrollment.

2.2.2. CMFA Verification

Continuous verification in the context of CMFA is a passive activity from the user's perspective. No overt authentication related action is required by the user to determine CMFA status. From the user's perspective, they are merely using the computer for its intended purposes. During the verification process, a user's CMFA verification input signals are periodically sampled by the CMFA TOE. The user is not prompted to provide any of these input signals. The TOE collects these data as needed from the computer/sensors whether or not the user is interacting with the computer. Each CMFA input signal is individually tested for quality and veracity according to each signal's defined standards as prescribed by the TOE vendor and selected by the CMFA Administrator. The CMFA engine calculates a score based on all authorized input data that meets prescribed data quality and veracity metrics to determine a Trust score. The Trust score, threshold value and possibly other relevant information is made available to the computer for use in determining security-related actions.

CMFA related signals include all the input signals available to the TOE as defined by the TOE vendor. Some or all available CMFA signals may be selected by the CMFA administrator for use in calculating the Trust score for a given use case. Data provided by these signals can include user biometric information, wireless signal information (BT, Wi-Fi, NFC, etc.), location, on body status, local time, various computer status information, information from external devices such as wearables that are paired with the computer, and others. CMFA signal selection may be static or dynamic. Static selections are made by the CMFA administrator and remain fixed until changed by the administrator. Dynamic selections are set by the administrator but can change according to changes in the computer status such as time of day, location, wireless signal strength, connected network ID, user request for change, etc. Limits on what is permitted to change and by how much are set by the administrator.

2.2.2.1. Verification Accuracy Measurement

An important consideration for any verification system is a measure of its accuracy. For comparison, biometrics systems are generally measured using FAR/FRR (or passwords are measured using length/complexity). The CMFA system though is not a single parameter used for authentication, but a combination of multiple inputs. As such the ability to provide a simple measure of accuracy such as the FAR/FRR for biometrics is not feasible, or even a good comparison between implementations.

2.3. CMFA Management

The configuration of CMFA is more complicated than single-factor authentication methods such as biometrics or passwords. Not only does it require the specification of the signals to be used by the CMFA Engine, the use of those signals must be configured. In addition to the configuration required by the administrator, the end user will need to provide training information (some of which may be collected over a period of time) to fully configure the CMFA for use.

CMFA management is expected to rely on the device management system to receive configuration policies. The device management system is relied upon to ensure the policy is trusted from the corresponding EMM. The actual CMFA policy on the device will be maintained within the SEE of the system.

2.3.1. CMFA Policy Settings

A CMFA policy would have a number of settings governing the overall configuration of the CMFA

Engine.

NOTE The options here are meant to be representative, but not exhaustive.

- Frequency of input checks (where applicable)
  - Separately determined for each input source
- Inputs to be used
  - Mandatory inputs
  - Optional/Selectable (per device capability) inputs
- Input configurations (examples below)
  - Trusted Wi-Fi network(s)
  - Trusted location(s)
  - Time period when usable
- Trust settings for inputs
- Score settings
  - parameters for combined inputs (i.e. location + time + Wi-Fi = good, vs just checking general parameters)
- Training parameters
  - Length of training needed
  - Forced user enrolment (where applicable)
  - Prompts for user information (such as entering location information, or adding biometrics)

2.3.2. CMFA Training

In addition to configuring the system settings, the user may have specific actions to perform to complete the enrolment process. Until the user has provided the training/enrolment/responses needed, the CMFA authentication template cannot be completed.

NOTE The options here are meant to be representative, but not exhaustive.

- Enrol a biometric
- Confirm a time zone
- Confirm a location (i.e. office/work location)
- Train a longer-term biometric (such as gait)
- Approve/confirm device connections (i.e. Bluetooth devices)

2.4. CMFA User Template Update

While the CMFA Training process performs the initial configuation of the user template, the CMFA system must also support explicit updates that may be outside the initial training window. These specific changes should not require a full training cycle to update the template (a shorter training cycle may be needed in some circumstances).

Some examples of changes:

- The user may enrol a new biometric (such as a new fingerprint, or an update to an existing fingerprint after an injury causes the original fingerprint template to no longer succeed)
- Selecting a new office location
- Changing a time zone (such as when traveling)
- Adding new Bluetooth devices

Similarly the admin may force a change in the template.

When making this type of change it is expected that the user would be required to provide a password/PIN to authorize the change of the template (as is required when changing a biometric template). To ensure proper security here, the changes would also have to be within a limited time window after the authentication.

NOTE At this time dynamic updating of the CMFA user template is not being considered, so changes to the template are discrete and require intervention from either the user or admin.

2.5. TOE Design

The TOE is fully integrated into the computer without the need for additional software and hardware. The following figure, inspired from [ISO/IEC 30107-1], is a generic representation of a TOE. It should be noted that the actual TOE design may not directly correspond to this figure and the developer may design the TOE in a different way. This illustrates the components that a CMFA system will rely on for enrolment and verification processes.

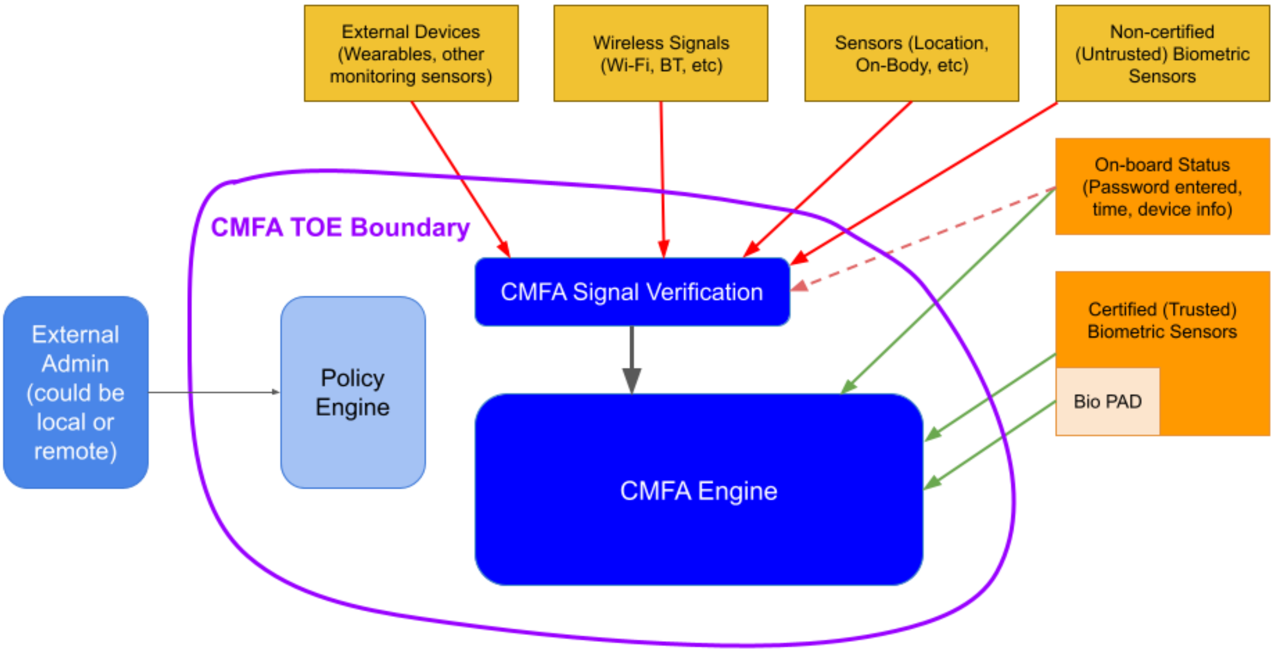
External Devices (Wearables, other monitoring sensors)
Wireless Signals (Wi-Fi, BT, etc)
Sensors (Location, On-Body, etc)
Non-certified (Untrusted) Biometric Sensors
On-board Status (Password entered, time, device info)
Certified (Trusted) Biometric Sensors
Bio PAD
CMFA TOE Boundary
CMFA Signal Verification
CMFA Engine
External Admin (could be local or remote)
Policy Engine

Figure 1. Generic representation of a TOE

As illustrated in the above figure, the TOE is comprised of:

- CMFA Engine - the core service of the CMFA that determines the authentication Score based on the user's profile (and will generate the profile during enrolment) based on the policy specified by the administrator
- CMFA Signal Verification - this filters input and associates Trust values with the incoming data. Additional processing may be done on an input related to the Trust value
- Policy Engine - this applies the configuration specified by the administrator (it does not perform any authentication processing)

Additionally there are external components used by the TOE:

- External Admin - this is how the administrator generates a CMFA policy (for example via an EMM or a special local app)
- External Devices - devices that may be attached to the computer (likely wireless, but could also be wired)
- Wireless Signals - wireless connections available to the computer such as Wi-Fi networks, Bluetooth or cellular (not exhaustive)
- Sensors (general) - sensors on the computer such as location, on-body detection, etc.
- Biometric Sensors (Trusted and Untrusted) - various biometric sensors that are available on the computer which may or may not be evaluated to the BIO-PPM
- On-board Status - information internal to the device such as time, special keys, etc

The lines between the external components and the TOE are representative to show:

- Red - external components that are untrusted and must be processed by the CMFA Signal Verification system before being passed to the CMFA Engine
- Orange dotted - possible status information from on-board the device that still may not be fully trusted and therefore must follow the same path as the external components
- Green - trusted components that are able to pass information directly to the CMFA Engine without being verified

The TOE verification flow can be represented roughly as this:

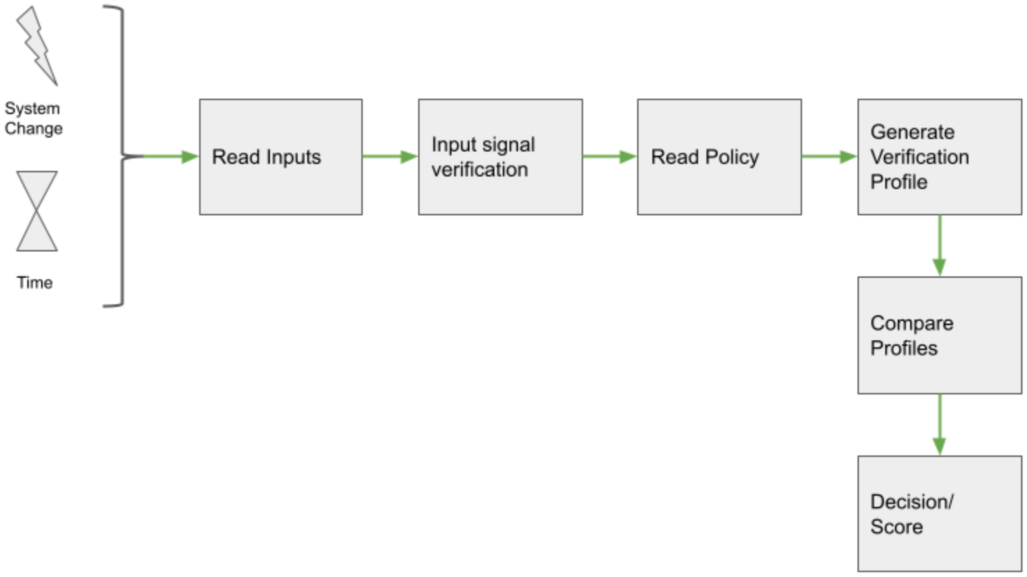

Figure 2. Verification flow

- Based on either time or a system change event (such as (dis)connecting to a Wi-Fi network), the CMFA will initiate reading of inputs (as specified in the CMFA policy)
- The inputs will be verified as needed
- The CMFA engine will check the current authentication policy
- Using the current policy a profile will be generated based on the collected inputs
- The collected profile will be compared to the stored user profile
- The CMFA engine will generate a Score and based on that value determine whether the user is still verified
- The decision and Score are made available to the main Operating System to determine any actions to be taken on the computer

An example of how a CMFA score would change over time can be seen here:

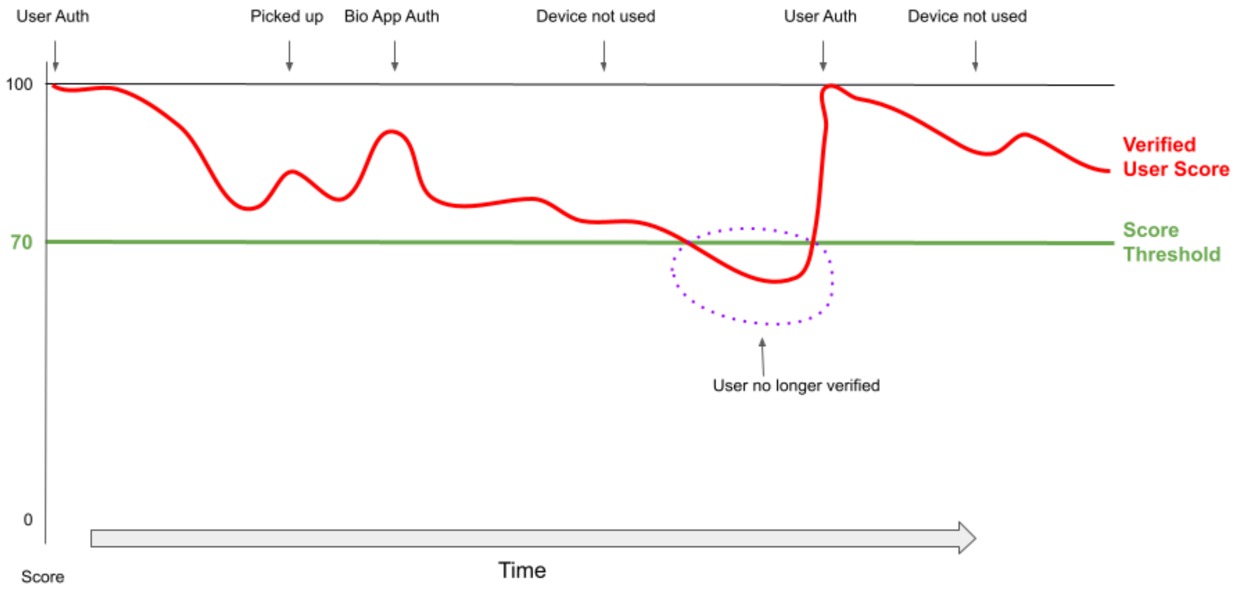

Figure 3. CMFA Score Timeline

2.5.1. Relation between TOE and Computer

The TOE is reliant on the computer itself to provide overall security of the system. This PP-Module is intended to be used with a Base-PP, and the Base-PP is responsible for evaluating the following security functions:

- Providing the NCAF (Non-Continuous Authentication Factor) to support user authentication and management of the TOE security function
- Invoking the TOE to enrol and verify the user and take appropriate actions based on the decision of the TOE
- Providing the Separate Execution Environment (SEE) that guarantees the TOE and its data to be protected with respect to confidentiality and integrity

The specification of the above security functions are described in the Base-PP and [PP_MDF Security Functional Requirements Direction] of this PP-Module.

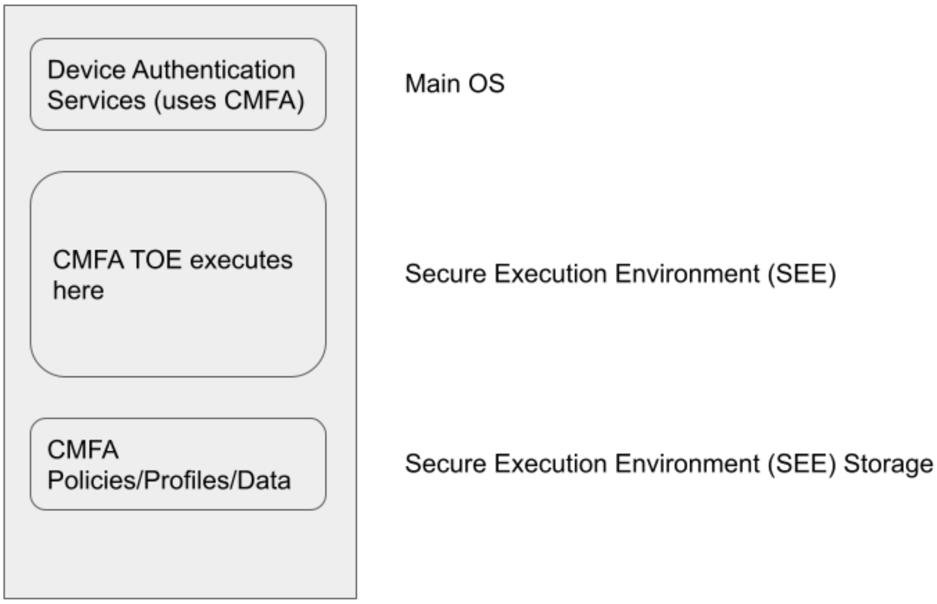
Device Authentication Services (uses CMFA)
Main OS
CMFA TOE executes here
Secure Execution Environment (SEE)
CMFA Policies/Profiles/Data
Secure Execution Environment (SEE) Storage

Figure 4. Generic relation between the TOE and the computer

2.5.2. TOE Use Case

The computer itself may be operated in a number of use cases such as enterprise use with limited personal use or Bring Your Own Device (BYOD). The TOE on the computer may also be operated in the same use cases, however, use cases of the TOE should be devised separately considering the purpose of biometric verification. The following use cases describe how and why biometric verification is supposed to be used. Each use case has its own assurance level, depending on its criticality a separate PP or PP-Module should be developed for each use case.

This PP-Module only assumes USE CASE 1 described below. USE CASE 2 is out of scope of this PP-Module.

2.5.2.1. USE CASE 1: CMFA verification for maintaining the unlocked state on the computer

This use case is applicable for any computers such as a desktop, laptop, tablet or smartphone that implement CMFA enrolment and verification functionality. For enhanced security that is easy to use, the computer may implement CMFA verification on a computer once it has been “unlocked”. The initial unlock is generally done by a NCAF which is required at startup (or possibly after some period of time), and after that, the computer lock state is maintained by the computer based on the Verified User Score as reported by the CMFA system and compared to the threshold score configured for the computer. In this use case, the computer is not supposed to be used for security sensitive services through the CMFA verification.

The main concern of this use case is the accuracy of the CMFA verification. Security assurance for computer that the TOE relies on should be handled by the Base-PP.

This use case assumes that the computer is configured correctly to enable the CMFA verification by the admin, who acts as the CMFA system administrator in this use case.

It is also assumed that the user enrols to the CMFA system correctly, following the guidance provided by the TOE. Presentation attacks during CMFA enrolment and verification may be out of scope, but optionally addressed. FTE is not a security relevant criterion for this use case.

2.5.2.2. USE CASE 2: CMFA verification for security sensitive service

This use case is an example of another use case that is not considered in this PP-Module. Another PP or PP-Module should be developed at higher assurance level for this use case.

Computers may be used for security sensitive services such as payment transactions and online banking. Verification may be done by the CMFA for convenience instead of the NCAF to access such security sensitive services.

The requirements for the TOE focus on the CMFA performance and presentation attack detection.

2.5.2.3. USE CASE 3: CMFA verification used to unlock external services

- for example using the score data to authorize unlocking a door

Chapter 3. Security Functional Requirements

3.1. TOE Environment Security Functional Requirements

The CMFA system is part of a larger environment (such as a mobile device), and relies on various services from that environment to provide some capabilities. There are three main areas that seem to be most likely to be relied that may have requirements that should be modified in a Base-PP (such as the PP_MDF_V3.3).

3.1.1. Audit (FAU)

The CMFA system itself likely would not have audit functionality built into the module itself, but should have various information included as part of the device audit system.

- enable/disable CMFA
- configuration update
- optionally record when the device locks (or unlocks if supported) based on Trust Score

3.1.2. Cryptopgraphic Operations (FCS)

The TOE is expected to rely on the platform for any cryptography, but at this time there are not any known functions that would require including FCS SFRs to the PP-Module.

3.1.3. Protection of the TSF (FPT)

The CMFA has its own requirements for this category, but may also rely on modifications to the Base-PP to provide support for securing the CMFA system and its data.

3.2. TOE Security Functional Requirements

This section lists SFRs that are proposed for inclusion in the PP-Module. Where a catalog SFR is available that has been copied here, otherwise the intent of an extended SFR is written out but has not been formally proposed (natural language vs CC requirement).

3.2.1. User Data Protection (FDP)

3.2.1.1. FDP_ACC.2 Complete access control

FDP_ACC.2.1

> The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects and objects*] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2

The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

3.2.1.2. FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1

The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

FDP_ACF.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

INFO: For the protection of data that is collected by the CMFA system the plan would be to use FDP_ACC.2. The point here is that the data that is collected by the CMFA is critical for privacy and so must be tightly controlled. This is explicitly on the data used internally by the CMFA, not on the input controls. For example location data on its own (from the location system) would not be subject to this, but once that data has come into the CMFA system, it needs to be protected by FDP_ACC.2.

3.2.1.3. FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] the following objects: [assignment: *list of objects*].

INFO: It isn’t clear how critical it is to have this requirement, and it is considered optional at this point. Given that the CMFA is supposed to be maintained in some sort of restricted environment, it may not be as important that data be cleared from memory during the use. Also, as the system is running continually, it also isn’t as clear how important this capability will be.

It is possible that this could be swapped for FDP_RIP.2, but it isn’t clear that is necessary (or feasible).

3.2.2. Identification and Authentication (FIA)

3.2.2.1. FIA_CME_EXT.1 CMFA enrolment

FIA_CME_EXT.1.1

The TSF shall provide a mechanism to enrol an authenticated user to the CMFA system.

INFO: To complete the enrolment of the CMFA system the user may need to enrol or acknowledge to various components of the system. For example the user may need to enrol a biometric or authorize the use of a biometric for CMFA. The user may also need to enter information like location info (or confirm it), or connect and mark accepted BT devices. The enrolment process for the user is unlikely to be a single step.

3.2.2.2. FIA_CMV_EXT.1 CMFA verification

FIA_CMV_EXT.1.1

The TSF shall provide a CMFA verification mechanism.

3.2.2.3. Template Configuration

SFR

The CMFA system can utilize the following inputs to create a template configuration: biometrics, location, etc. The input requirements/constraints shall be defined.

INFO: While it is expected that any biometric used by the CMFA should have been evaluated to the Biometrics PP-Module, this is not actually a requirement. The constraint would be the level of trust allowed based on whether the biometric has been evaluated or not (only an evaluated biometric could be considered "trusted"). Another example could be the power on the radio that is needed to be used (for example a signal of at least XYZ dB).

SFR

A template configuration shall require that the calculated trust score would be comprised of at least 2/3 value from trusted input signals.

INFO: The point here is that a template configuration will be used to generate a trust score that will be used by the system to determine the unlock status. The calculation of the trust score uses weighted values for the different inputs, and untrusted inputs should not count for more than 1/3 the total score.

3.2.2.4. Template Quality

SFR

The quality of the CMFA template must be sufficient to ensure the accurate identification of the authenticated user over time. The CMFA template must be composed of at least 3 signal inputs.

INFO: The question here is whether or not there should be separate enrolment and verification requirements (as with biometrics). This is in part a question because enrolment will take time, so it is not quite a point-in-time period which would provide higher assurance about the enrolment quality.

The template must be composed from at least 3 signal inputs, but more are allowed, this is just the absolute minimum allowed by the PP-Module.

3.2.2.5. CMFA Signal Verification

SFR

The TSF shall perform user verification on a defined periodicity and report the resulting score to the authentication system.

INFO: This requires the system to define the method for performing the periodic checks (the time period may be fixed by the vendor or set by the admin).

SFR

The TOE shall prevent the use of artificial attack signals from being used in the verification process.

INFO: The idea here is that the attack detection is on individual input signals to the CMFA system and not to the whole of the final calculation.

Attack detection may be optional, but if it could be used on select signals as opposed to all it could be mandatory. For example location may have detection, but time may not. Inputs that have their own attack detection (such as biometrics including PAD) would not need additional checks. If this is mandatory but flexible, a minimal set of signals may be specified as mandatory to have checks (if the input signal is supported by the system).

3.2.2.6. CMFA Score

SFR

The TOE shall combine the input signals to generate a score based on the template configuration that will be reported to the authentication system.

3.2.3. Security Management

3.2.3.1. Management Functions

FMT_SMF.1 & FMT_MOF.1

This combination would specify a set of management functions and provide for them to be divided between the admin and user.

The following types of management functions would be available:

- Admin
  - enable/disable
  - input signals to be used
  - configuration of input signals (i.e. office location, office Wi-Fi network)
  - enrolment period
  - frequency of input checks (for example static with fixed periods or dynamic where the

    - frequency may change based some parameters)
    - enrolment period use (can the system be used for verification before the end of enrolment or not)
    - trust settings for input signals (score weighting)
- User
    - allow use of biometrics
    - enable/disable (if admin allows use, user can choose to not use, or stop using)

INFO: For options like the enrolment period, this could vary with being for the entire profile or just select components (for example gait, which may take longer to accurately model)

3.2.3.2. FMT_MSA.2 Secure security attributes

FMT_MSA.2.1

The TSF shall ensure that only secure values are accepted for [assignment: *minimum secure configuration requirements*].

INFO: The point for this would be to specify the minimum input signal requirements necessary to configure CMFA. This is tied with CMFA template quality proposed SFR.

3.2.3.3. FMT_MSA.4 Security attribute value inheritance

FMT_MSA.4.1

The TSF shall use the following rules to set the value of security attributes: [assignment: *rules for setting the values of security attributes*].

INFO: Something like this SFR would be used to specify the trust settings for the inputs for CMFA. Likely this would need to be extended (given the dependencies here not making sense), but this would be the general ideal to set this information.

3.2.4. Privacy

SFR

The CMFA template shall not be exported.

INFO: There isn't an exact requirement for this, and it could be done not with a privacy requirement. There are some MDF requirements that may be able to be used for this, but the purpose of this statement is that the template, which will hold a lot of personal data, shall not be able to be exported from the device to ensure this data is protected.

3.2.5. Protection of the TSF (FPT)

3.2.5.1. FPT_CDP_EXT.1 CMFA data processing

FPT_CDP_EXT.1.1

Processing of plaintext CMFA data shall be inside the SEE in runtime.

INFO: The expectation here is that the SEE also provides protection for data at rest to ensure that any information that is stored cannot be accessed in that state.

3.2.5.2. FPT_PCT_EXT.1 Protection of CMFA template

FPT_PCT_EXT.1.1

The TSF shall protect the CMFA template [**selection**: *using a PIN as an additional factor, using a password as an additional factor*, [**assignment**: *other circumstances*]].

3.2.5.3. FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: [*when the CMFA system detects invalid inputs*].

INFO: The purpose of this requirement is that if invalid inputs (or other possible conditions that may be critical, such as the system crashing), would fail over to the normal authentication mechanism. Basically the point would be that in the case of a "critical" failure, the score would go to 0.

3.2.6. Trusted Path/Channels

3.2.6.1. FTP_TRP.1 Trusted path

FTP_TRP.1.1

The TSF shall provide a communication path between itself and [*local*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [*modification*].

FTP_TRP.1.2

The TSF shall permit [*the TSF*] to initiate communication via the trusted path.

FTP_TRP.1.3

The TSF shall require the use of the trusted path for [[*list of input signal sources to the TOE*]].

INFO: Trusted path here is to ensure a secure channel between the input signal and the CMFA system. Disclosure of the data is not really a concern here, though this could be useful from a privacy standpoint (again because the data collected for CMFA is really personal). The source of the signal over the path can also be used as a determination of trust of the input. Since some signals may come over what may be untrusted channels, this is likely an input into determining the trust level that can be assigned to the input.