FeliCa Approval for Security and Trust (FAST) Overview

FeliCa Networks

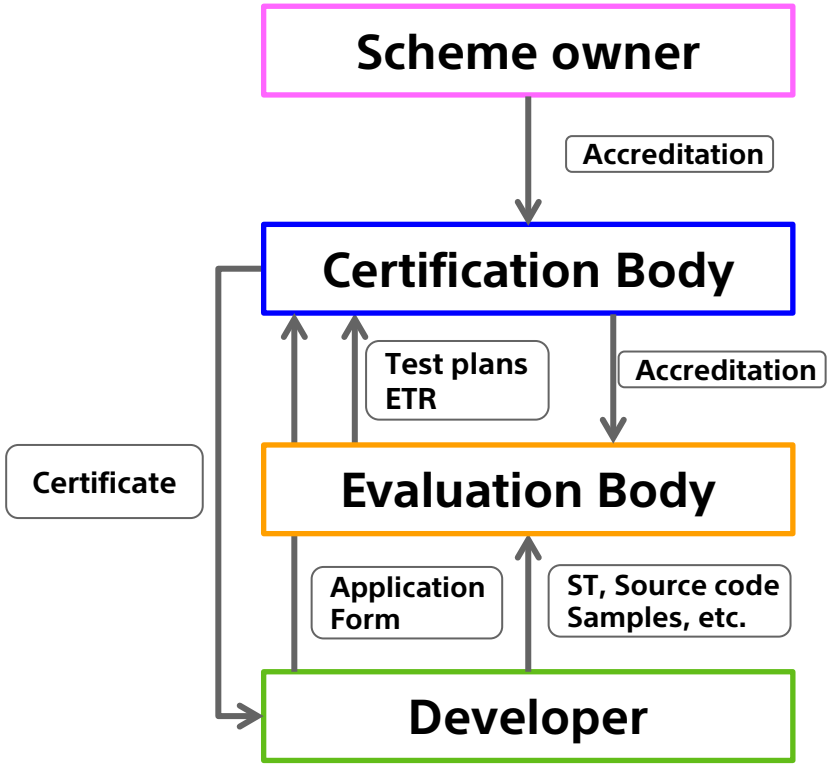
Introduction

- The security certification scheme called “FeliCa Approval for Security and Trust (FAST)” has been set up to enable the evaluation and certification of the mobile FeliCa product security aspects.
- The FAST scheme is driven by the independent certification body and the certificate is issued as ISO/IEC 15408 (Common Criteria) certificate.
- The TOE are FeliCa Card product that consists of the security IC and FeliCa OS, and Mobile FeliCa product that consists of the Security IC, the operating system (such as Java Card OS), and the mobile FeliCa application (such as payment and transit applications) including relevant crypto libraries for AES.
- The FAST scheme aims to give a high assurance of security level (i.e., AVA_VAN.5), in a timely manner, to the service providers who deploy FeliCa products for their payment and/or transit services.

Intent

- The intent of the scheme is to provide sufficient assurance for the certified products to protect the assets against potential threats.
- This scheme streamlines the process by focusing on specific threats that FeliCa products are exposed to.
- To maintain a consistent and state-of-the-art level of assurance, while reducing the time and cost of certification management, a streamlined certification process is defined.
- In this certification process, an ISO/IEC 17065 accredited certification body shall assess the evaluation results, and shall then determine whether the products provide sufficient assurance to be certified under this scheme.

FAST roles and responsibilities



FAST v2 and FAST v3

	FAST v2	FAST v3
Security evaluation method	ISO/IEC 15408(CC) ISO/IEC 18045(CEM)	
EAL	FeliCa Card EAL5+, EAL6+ FeliCa Applet EAL4+	FeliCa CL and FeliCa Applet EAL4+
PP	FeliCa Card: Public Transportation IC Card Protection Profile FeliCa Applet: Mobile FeliCa Applet Protection Profile	FeliCa CL and FeliCa Applet : Mobile FeliCa Applet Protection Profile
Certification body	TrustCB	
Evaluation body	Applus+, Brightsight, ECSEC, Keysight SERMA, TUViT	
Evaluation style (Card)	Product certification Composite certification (Either CC or EMVCo certification is required for the Platform TOE)	Out of scope
Evaluation style (FeliCa Applet/FeliCa CL)	Composite certification (Either CC or EMVCo certification is required for the Platform TOE, and FAST certification is required for the FeliCa CL.)	Composite certification (Either CC or EMVCo certification is required for the Platform TOE, and FeliCa Applet has been evaluated in advance.)
Valid period	Five years (Can be extended by five years through the renewal process)	

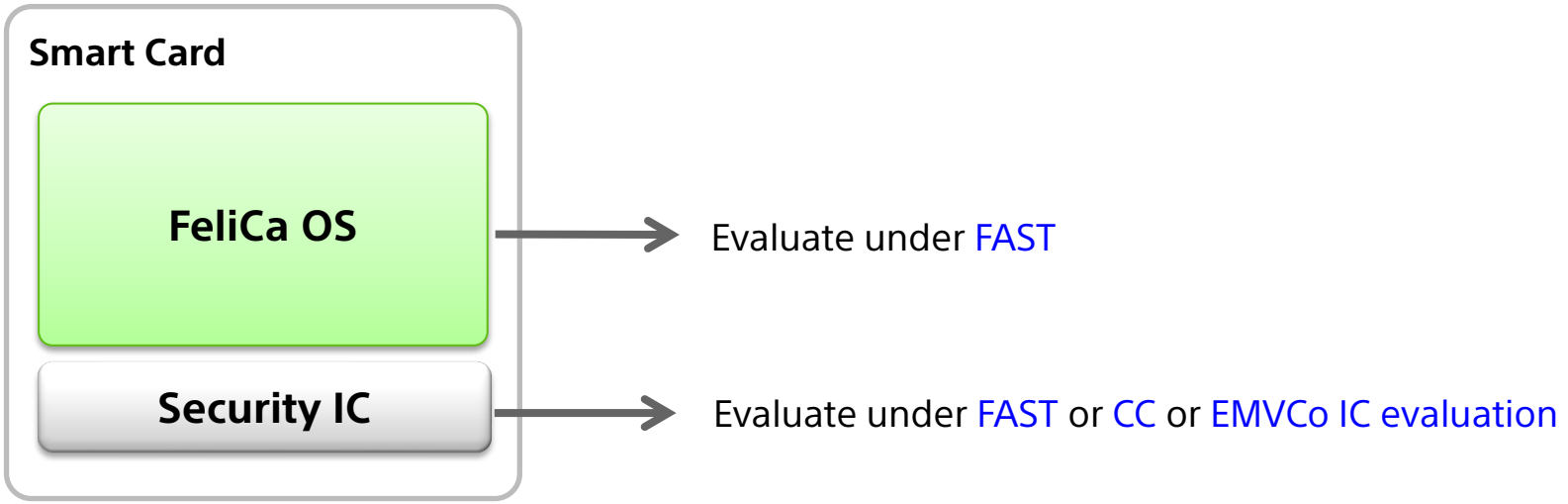
Conditions for the FeliCa CL application

Basically, the scheme owner defines the FAST scheme policy as follows, so if there are any changes in the TOE, FeliCa CL vendor needs to apply for FAST v3. However, depending on the individual situation, it may be more appropriate to conduct maintenance or recertification under FAST v2.

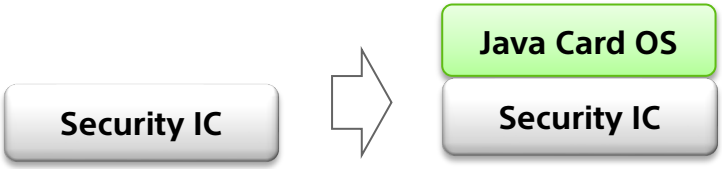
FAST v2	FAST v3
Recertification of FAST v2 existing certificate and TOE doesn't have any changes (i.e. Recertification to extend the validity period)	New certification, or Recertification or maintenance of FAST existing certificate.

FAST v2 scope and process (FeliCa card)

Certification scope



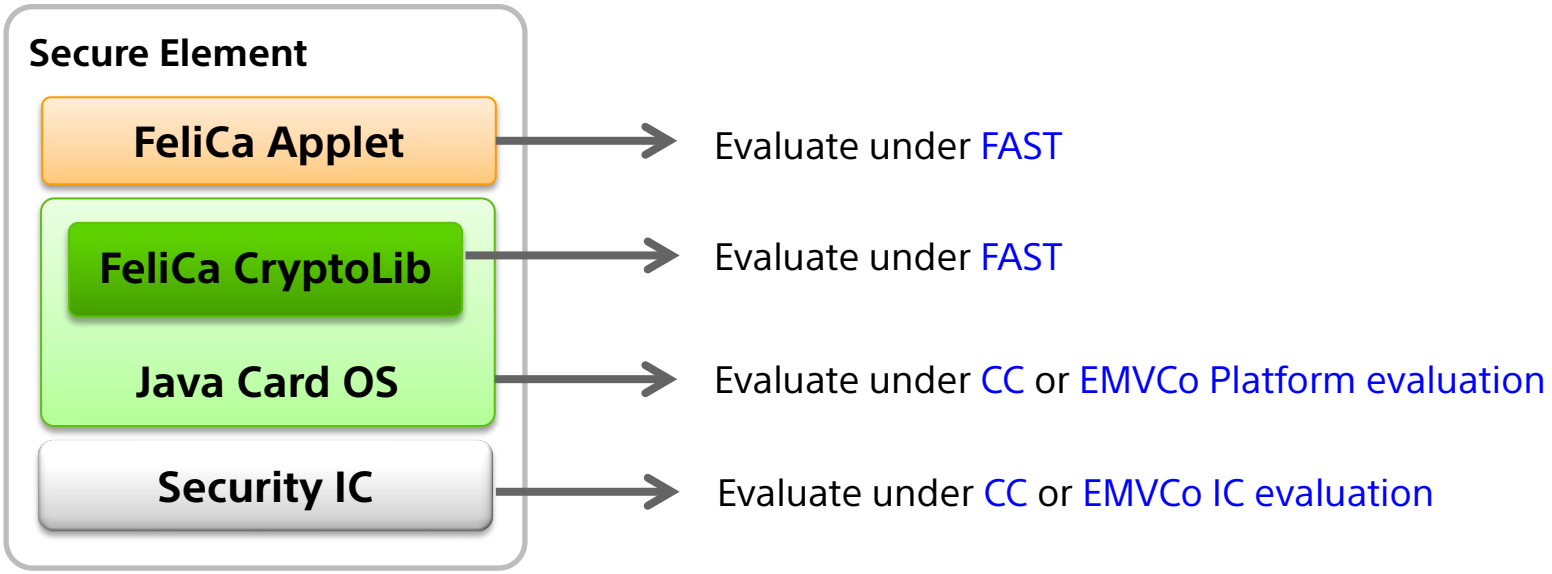
Composite certification process



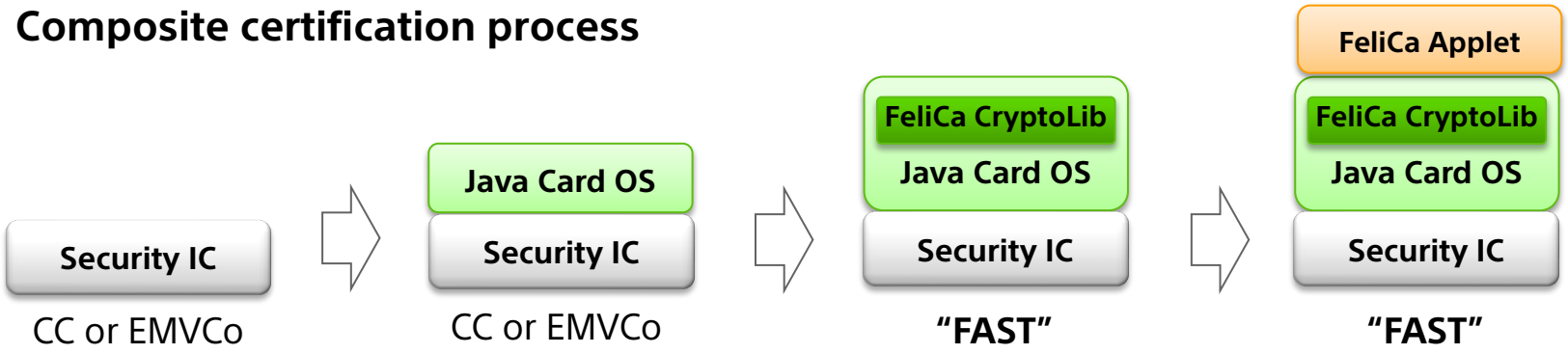
Product certification process

FAST v2 scope and process (FeliCa Applet)

Certification scope

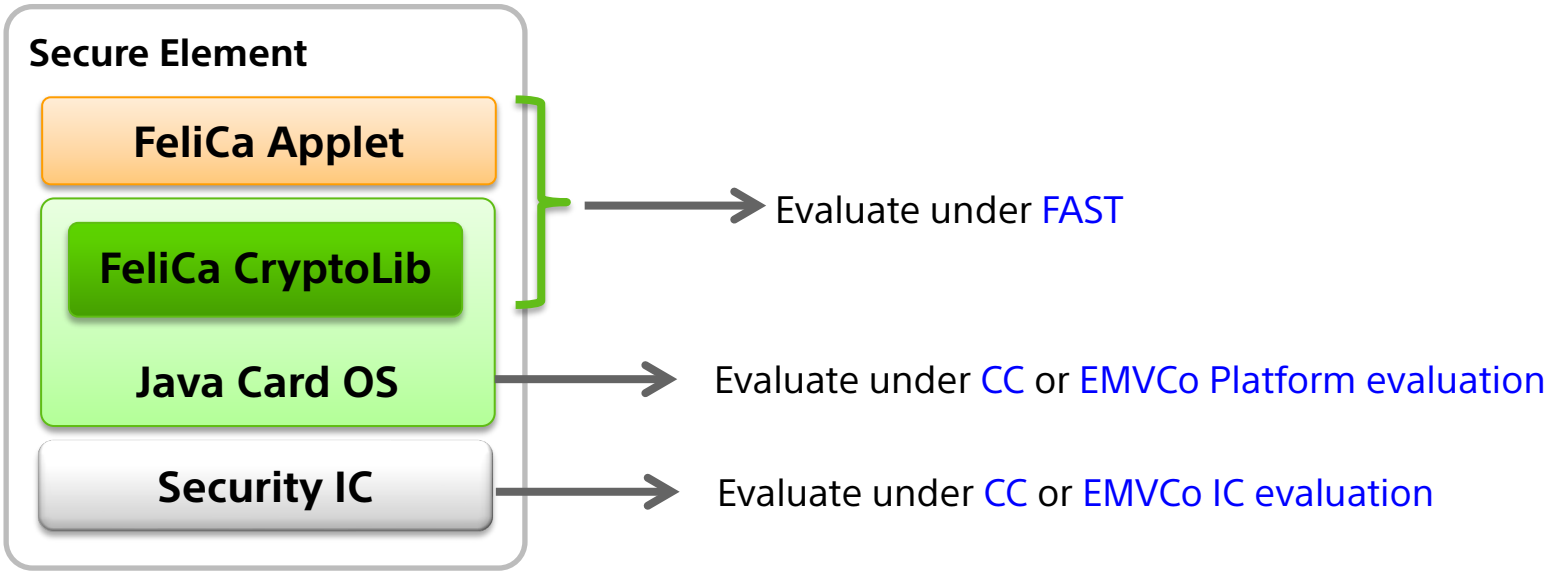


Composite certification process

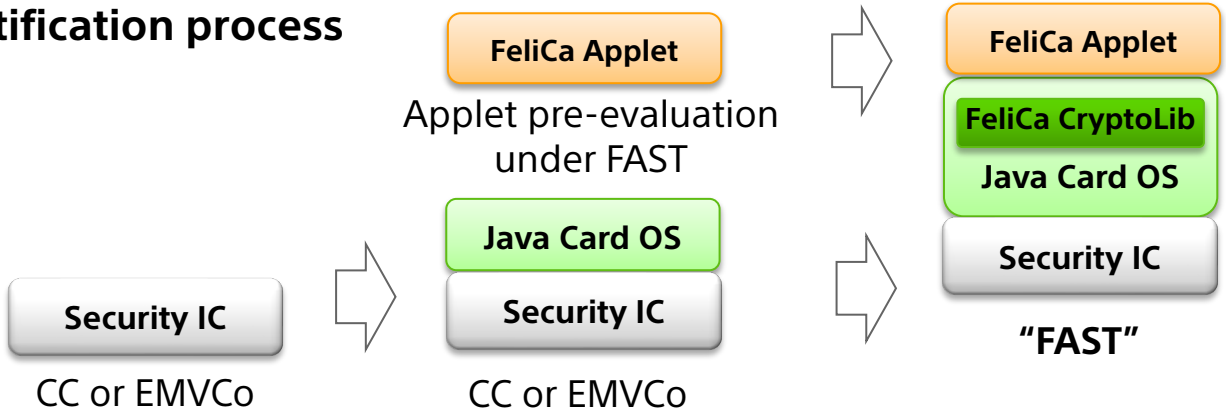


FAST v3 scope and process (FeliCa CL and FeliCa Applet)

Certification scope



Composite certification process



Requirements (non-exhaustive list)

- All requirements for evaluation and certification are defined in the scheme document “FeliCa Approval for Security and Trust scheme v2” or “FeliCa Approval for Security and Trust scheme v3” provided by the certification body.

- Key evaluation aspects:
  - TOEs are evaluated according to ISO/IEC 15408 (CC) and ISO/IEC 18045 (CEM)
  - Penetration test against high attack potential (AVA_VAN.5)
  - Site security (EMVCo site audit or the site certification under CC scheme can be reused)
  - AES crypto protocol

- Certification validity
  - 5 years
  - Validity can be extended by 5 years through the renewal process