White Paper: CAST

MasterCard CAST Approval Process for Secure Element Based Mobile Payment Applications

Introduction

The CAST (Compliance Assessment & Security Testing) process for Mobile Payment Applications has been improved to take advantage of the online nature of mobile devices and their capability for post issuance download of applications into Secure Elements. This differs slightly to the CAST model for traditional smartcards. It is the intention of this white paper to explain the differences and the new process impact.

Summary: CAST Process for Mobile Payment Applications

The advent of mobile devices with increased online connectivity has given rise to the ability to modify applications more easily after they are issued. The CAST process has been updated to respond to this industry change.

By reviewing the CAST policy on backdating approval issue dates, Mobile payment products that successfully demonstrate state of the art security when full evaluation testing has been performed will be considered as new products, qualifying for a 3 year CAST certificate with a new issue date provided the vendor uses the original security evaluation laboratory and the underlying platform is maintained under the EMVCo security evaluation programme. This process is termed a Refresh Evaluation.

This change also makes possible the alignment of CAST approval expiry dates across different payment products on the same underlying platform and thus maximises the platform's time in the field, so removing the conflict over withdrawing the product early because different Apps are loaded at different times.

Benefits for Payment Product Developers:

- Refresh evaluation leads to a new 3 year approval
- Refresh testing can be conducted prior to product launch to maximise the product lifecycle, thus removing the time consumed with product preparation and testing by the Mobile Network Operator and Financial institution prior to product launch
- Refresh testing required for Issue date refresh is achieved in a short time due to limited evaluation scope at the application level
- A refresh evaluation easily extends the product lifecycle supported by additional security assurance
- As new security threats develop, the refresh approval process encourages applet level fixes resulting in the most secure and feature rich product also benefiting from a new 3 year approval
- Delta payment products receiving full application level testing will also benefit from a new 3 year approval period. This includes updates due to specification changes
- A developer managing multiple payment products on the same platform can obtain aligned approval and thus aligned expiry dates. For example, regardless of when the CAST approvals are granted, performing a final refresh prior to PCN expiry will align all CAST expiry dates (3 years from PCN expiry). Note: If other payment systems were to adopt this approach, the expiry dates would align across all payment systems
- Aligned payment product expiry dates give rise to a simplified product portfolio management should further refresh evaluations or renewal evaluations be required
- No limit exists on the amount of refresh evaluations that can be conducted. The only requirement is that the underlying platform (specific OS on a specific IC) and the IC (Integrated Circuit) remain EMVCo maintained and the CAST approval does not exceed 12 years.
- Applet level refresh testing remains an option for products that continue to be maintained with security testing at the IC/Platform level even if the EMVCo approval has expired. See the EMVCo Security Evaluation Process document for more information on the expired IC/Platform product extension process.

Benefits for Mobile Network Operators:

- Product lifecycle is extended
    - Possible to receive up to 12 years CAST product approval
    - Possible for the Secure Element with a Specific Payment Application to remain valid in the field for up to 15 years when a 3 year credential expiry is used
- Multiple payment products from different product developers using the same platform can obtain aligned approval and thus aligned expiry dates
- Aligned payment product expiry dates give rise to a simplified product portfolio management and a clear forecast for USIM (Universal Subscriber Identity Module) migration requirements
- Security assurance is demonstrated for products obtaining a long lifecycle

- Functionally updated or security patched applications benefit from a new 3 year approval thus encouraging issuer migration to the latest and most feature rich payment application product
- Payment applet fixes/updates do not impact other application present on the product
- Renewal testing remains an option for products when the EMVCo platform is no longer maintained or approved.

Benefits for Financial Institutions:

- Possible for the Payment Application to remain valid in the field for up to 15 years when a 3 year credential expiry is used, this would increase further should the financial institution decide that a longer credential expiry is acceptable
- Latest functionality enhancements and latest security applied at the applet level is received by the issuer / end user (device holder), thus benefitting from the most secure and feature rich product
- Confidence in 3 years product approval prior to product launch.
- Applications can be activated in the field for this 3 year period and the possibility of further refresh testing to obtain a new 3 year approval at any given time whilst the underlying IC and platform remain EMVCo maintained.
- Refresh testing remains an option for products when the IC/Platform is no longer approved but continues to be security evaluated by EMVCo. See the EMVCo Security Evaluation Process document for more information on the expired IC/Platform product extension process.
- Financial institution retains control for the decision on application expiry
- Multiple payment applications having the same expiry date ensure aligned product migration requirements for all financial institutions. This can be either multiple payment products for a single financial institution or multiple products on the same platform from several financial institutions

More Details On The Process

CAST Objective

The CAST process requires all product vendors to submit their product to an independent CAST approved laboratory for a security evaluation. This laboratory will perform a CAST evaluation (Vulnerability analysis / Penetration testing) against the latest CAST security guidelines and submit a security evaluation report to CAST. If the product defences have been sufficiently demonstrated, the product will not have any identified security vulnerabilities and a CAST approval will be granted.

CAST Approval Lifecycle Management

From an issuer perspective, the most important part of the CAST approval is the approval certificate number (CCN / MPCN etc) and its associated issue date. The CAST approval is valid for 3 years from the CAST approval issue date. It is therefore important that the issuer understands the associated lifecycle when selecting a suitable product.

It is a critical part of the CAST process that the approval date reflects the date when the evaluation work was completed as this reflects the state of the art in security testing at this point. As time progresses, attackers discover new techniques and their equipment becomes more powerful and cheaper mirroring Moore's Law. Because of this the security of any product decreases over time.

It is with this in mind that CAST will occasionally backdate an approval so the date accurately reflects exactly when the security assurance was derived. This can be for several reasons, for example: Reuse of evidence from a previous evaluation / delta review as the product is derived from a parent product / delay brought about by rework / long period between report completion and submission to CAST etc. The most common reason for backdating is due to the product being derived from an older, parent product.

The introduction of Mobile Payment products has changed the way we look at security compared with the traditional smartcard model. For the traditional chip based bank card, the card is shipped in its final configuration to the end user (device holder), and it is not possible for the card to receive further applications once it has been issued. For most of its life, when not being used to make a face to face purchase in a terminal, it remains offline in someone's purse or wallet.

For a mobile payment application to be personalised into a Secure Element (SE), the product is not in its final configuration when it is delivered to the end user (device holder). The SE needs to be able to receive applications whilst in the field. Since the SE resides in a mobile device, it is likely that the majority of its life will be spent in an environment with frequent online connectivity, even when not in a face to face payment situation.

The additional complexity of these post-issuance download capable SEs has almost tripled the evaluation effort required, for example in a USIM product. However, because of its online capability, which offers the chance for more frequent updating of Mobile Payment Applications, this offers the chance to maintain the security of the product whilst in the field.

Leverage the EMVCo IC and Platform Approval Process

The current evaluation model for a mobile payment SE product is to start with the IC evaluation and approval via EMVCo. The operating system is then loaded and evaluated through a separate EMVCo platform process. Assuming the security review is successful, the open platform approval is obtained from EMVCo, and this means the approved products are able to be used for **new** composite products. The EMVCo approval for the IC and platform is valid for 1 year, so in order to keep the IC and platform on the approved products list, a renewal evaluation must be conducted each year, for up to a maximum of 6 years. It is still possible for an IC/Platform provider to support the device further with the EMVCo process, the additional security evaluation work does not result in an extended approval but it does allow the reuse of evaluation evidence from the IC/Platform to facilitate the composite CAST refresh or renewal evaluation. It should be noted that the IC and platform evaluation provide the majority part of the security assurance that will be reused by a composite product.

CAST Applet Level Approval for SE Based Mobile Payment Products

Loading a MasterCard payment application onto an EMVCo approved mobile platform product will require a CAST evaluation resulting in a report submitted to the CAST team for review. If the product security defences have been sufficiently demonstrated, the product will receive the CAST approval. The CAST approval will remain valid for 3 years (Assuming a new attack is not developed that compromises the product security) after which a renewal evaluation can be performed, again, if successful, a further 2 year approval will be granted. The renewal process for CAST can be repeated to achieve an overall approval time of 7 years from the CAST certificate issue date. It should be noted that a Refresh Evaluation may be performed at any time and if successful, a new CAST approval issue date will be granted, so the 7 year approval may be obtained from the new issue date. As an example, if a product received CAST approval with an issue date of 1st Jan 2014, if a refresh evaluation is performed 2 years later, the new CAST issue date will become 1st Jan 2016, thus the 7 year CAST lifecycle would apply from 1st Jan 2016. One limitation exists here, the CAST approval per product cannot exceed 12 years – See Figure 3. Once the approval period has ended, further personalisation of applets in the field would not be permitted, however, applets already personalised in the field will remain valid until the applet expiry date is reached. The following figure illustrates the Application renewal timeline, where FE stands for Full security Evaluation for the new product, and DE stands for the Delta security Evaluation for the renewal of the product.

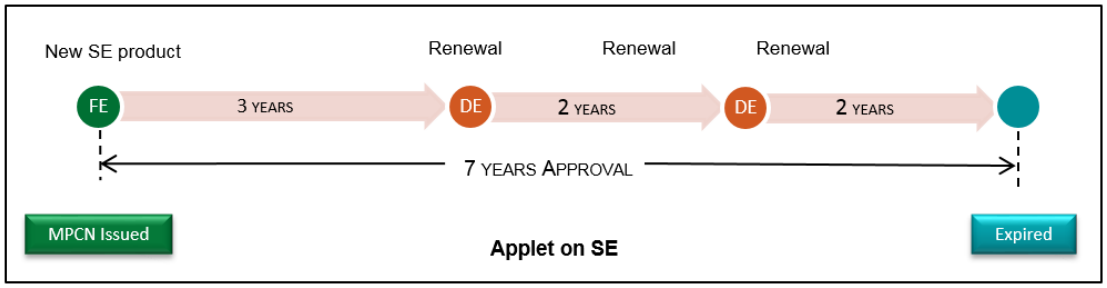


Figure 1 – Application level Lifecycle

Refresh Evaluation for Mobile Apps on a Post Issuance Capable Platform

Once the CAST approval for a specific application on secure element product has been obtained, it will be possible to refresh the CAST approval issue date by performing a full set of CAST testing (termed – Refresh Evaluation). This means that a product that obtained its CAST approval on the 1st Jan 2014 could undergo a full CAST evaluation the following year and the CAST issue date would be brought forward to the new evaluation evidence date, 1st Jan 2015. The certificate would then be valid for 3 years from the new issue date. A further 2.5 years later, another refresh evaluation may be performed, assuming successful, this would result in a new CAST certificate issue date of 1st July 2017. The only requirements are that the original evaluation laboratory must conduct the evaluation (this brings the benefit of the lab's previous experience to the new evaluation) and the underlying platform must be security maintained under the EMVCo process.

It should be noted that the maximum CAST approval for a mobile applet on an SE product is 12 years. This extended lifetime can be achieved with the refresh process alone or a combination of the refresh process and the renewal process.

CAST for Mobile Payment Products vs Traditional Smartcards

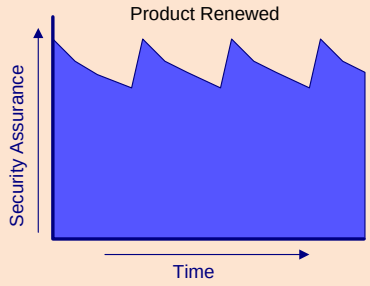
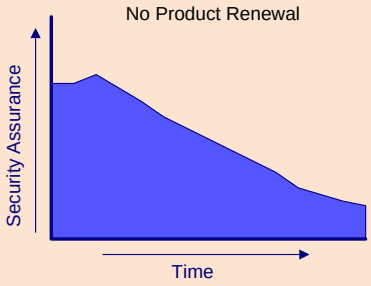
Action	Mobile Payment Product	Traditional Smartcard
Yearly Renewal for Platform and IC	The MPP underlying platform will undergo a yearly renewal via EMVCo	Once the product is evaluated and approved, no further work is usually performed to refresh the security approval of the underlying platform
		
Product updates in the field to accommodate new security threats	The MPP is easily deleted in the event of a field issue, so the applet can be removed and replaced with a new improved applet within a very short time	Products issued into the field are extremely difficult to recover and replace on a large scale should a field issue be identified
New Issue date to be applied to the CAST approval for the MasterCard banking application product undertaking a refresh evaluation	Full testing at the applet level will be required using the original security evaluation laboratory, this provides current evaluation evidence of which the updated issue date will be derived	If the same refresh testing was to be performed for a traditional smartcard, this would not be acceptable for a CAST approval issue date refresh, the reason is related to a smartcard not being able to change the application or fix a bug for a product in the field, this brings "time in the field" as a security vulnerability back into play.
Alignment of the CAST approval expiry date for a multi "payment application" product (When issuance of payment applications must cease)	The alignment of product approval has been a big issue for Mobile payment products. Since a single mobile payment product can host a number of payment applications and a number of additional applications, the expiry of 1 application is not sufficient to trigger the rollout of a new mobile payment SE platform to the end user (device holder), thus alignment of the product expiry for security is required	A Bank issuing traditional smartcards will generally issue with 1 payment application and a predefined set of additional application that has been evaluated as part of the CAST evaluation. The bank has total control of this product, ie: knows when the product is issued and activated. The alignment of the CAST approval expiry date is not relevant. The bank simply migrates to a new product when ready.

Table 1 – Comparison of Smartcard and Secure Element Products

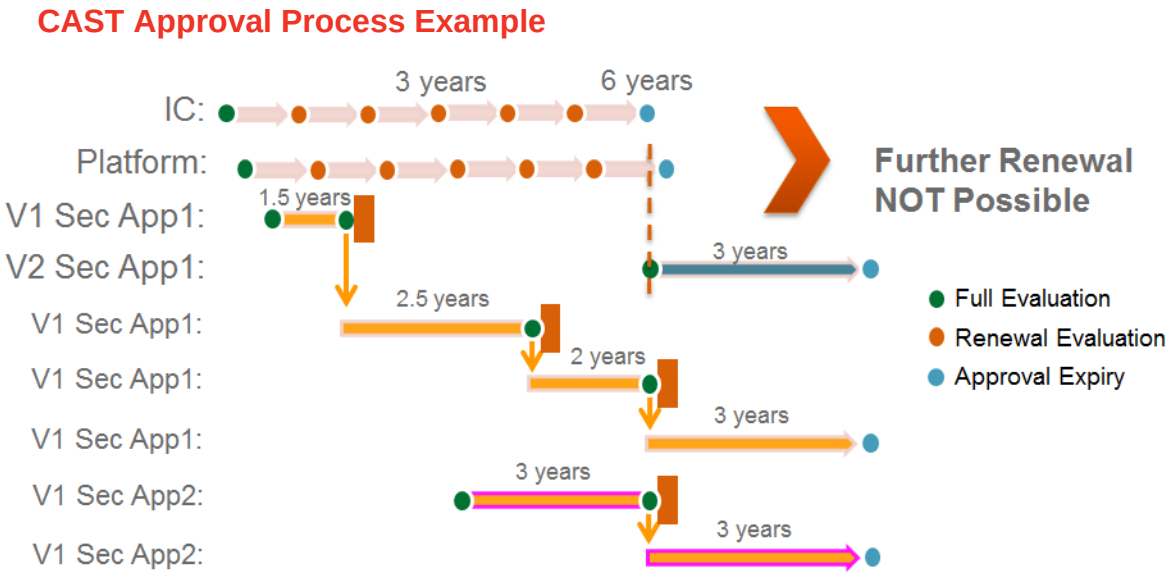


Figure 2 – New model for Mobile Payment Products

As can be seen from figure 2, the IC and platform approval is possible for the full 6 years following successful yearly renewal evaluations. For Vendor 1 secure payment application (V1 Sec App1), the original CAST approval is obtained shortly after the EMVCo platform approval, giving rise to the 3 year CAST approval. V1 always has the option to perform a renewal evaluation at the end of the 3 years, however, as the application specifications are likely to have changed (based on our experience to date) the best course of action would be to get approval for an updated product. So by allowing the same product or variant product to have a refreshed CAST approval issue date means that Vendor 1 can get the maximum use of the underlying platform and also maximise the product life in the field.

Important Note: Figure 2 above covers the approval period for a CAST approved product. Throughout the approval period, product activation in the field is permitted. Once the approval period has lapsed, product activation in the field is no longer permitted. When a product is activated in the field, the product will be personalised with an expiry date (Duration decided by the product owner), that will allow the product to remain active in the field in addition to the approval period. MasterCard recommends a 3 year credential expiry period to be used.

As an example in Fig 2, V1 Sec App1 is approved shortly after the platform has been approved. If after 1.5 years, the vendor performs a full application level evaluation a new CAST approval issue date is obtained. This process can be repeated so that V1 can have a 3 year product approval just before the platform and IC expire. This means that V2 and V1 now have the same approval expiry date. The credential expiry date applied when personalising the product will be additional time in the field.

Using this process, it can be seen that an IC can be in the field for up to 10 years plus the decided applet expiry period (usually 3 years). In fact, V1 or V2 may choose to perform a renewal evaluation to extend their CAST approval further (See Figure 1). The vendor would need to evaluate the IC, OS and application as a single product in order to extend the CAST approval. This is due to the IC and platform renewal no longer taking place, so the Application level product evaluation would need to consider this additional work.

CAST Approval Process Example – Extended Refresh

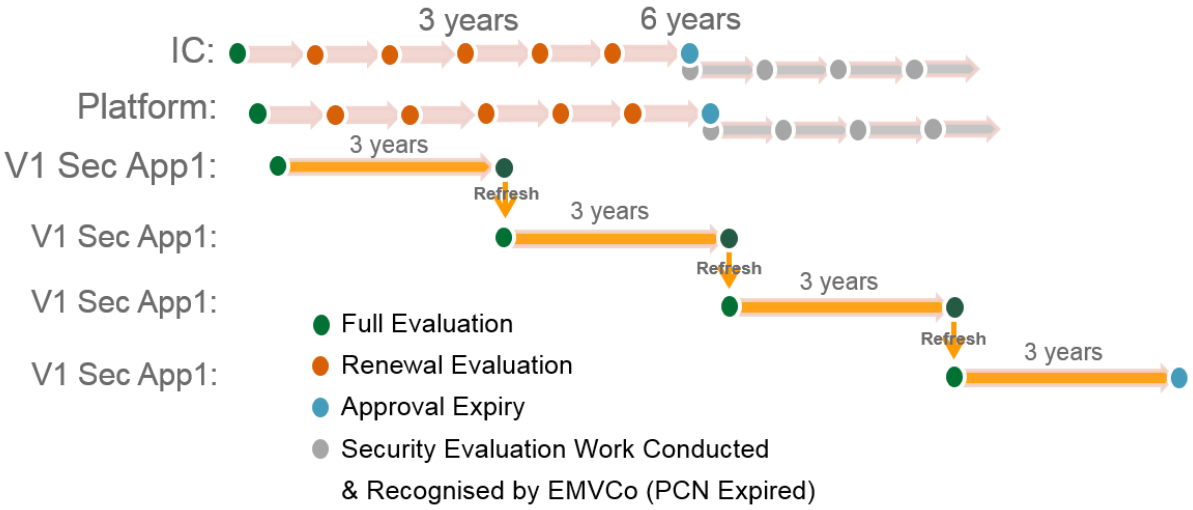


Figure 3 – Refresh on Expired Platform

As can be seen from figure 3, the IC and platform approval is possible for the full 6 years and the IC/Platform product providers continue to perform the yearly security evaluations, accepted by EMVCo to fulfil the composite reuse of evidence requirements. For Vendor 1 secure payment application (V1 Sec App1), the original CAST approval is obtained and the refresh evaluations are performed on a 3 year cycle reaching the maximum 12 years CAST approval. At this point a further refresh or renewal evaluation is not permitted.

It should be noted that a brake in the IC or Platform EMVCo approval/recognition will void the use of a refresh evaluation for CAST.

CAST Approval Process Example – Refresh & Renewal

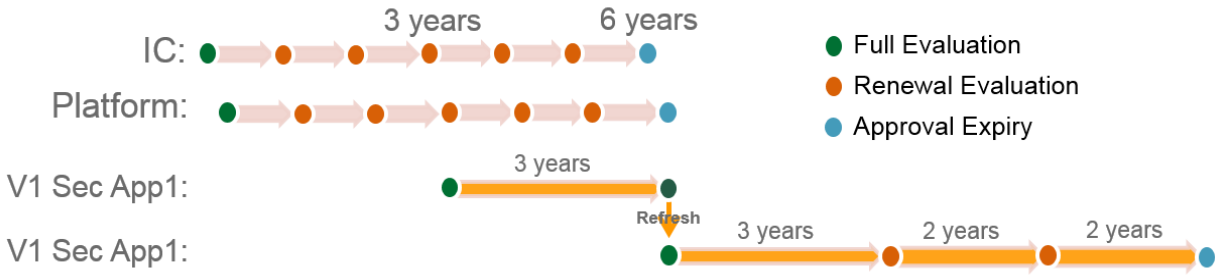


Figure 4 – Refresh & Renewal

In figure 4, the IC and platform approval is achieved for the full 6 years but the IC/Platform product providers do not continue the yearly EMVCo security evaluations. For Vendor 1 secure payment application (V1 Sec App1), the original CAST approval is obtained along with a refresh evaluation that obtain 6 years of CAST approval. The product owner wishes to extend the life of the product further so a renewal evaluation is performed. Since the IC and Platform have not been supported, the Applet level renewal evaluation must include the Platform and IC within the vulnerability analysis and conduct the corresponding penetration testing as required. After 2 years the above process must be repeated to achieve the second renewal.

CAST Approval Process Example – Security Assurance Level

Figure 5 below provides an example of the security assurance derived from an EMVCo / CAST maintained product. It can be seen that the High assurance level is almost constantly maintained due to the IC renewals, Platform renewals and Applet level renewals. It is this additional assurance and the Mobile phone flexibility that gives rise to the mobile products receiving a new issue date when the refresh evaluation is achieved.

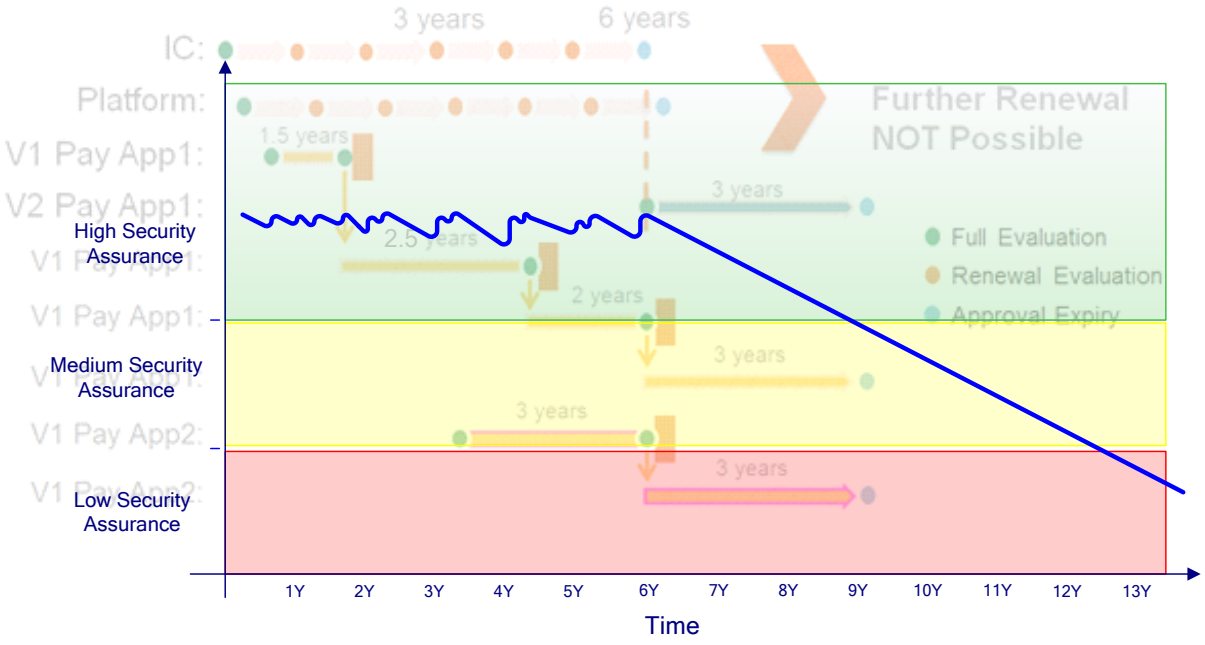


Figure 5 – Mobile Product Security Assurance Level

Figure 6 considers the SmartCard approval, showing the security assurance falling over time and reaching a low level of assurance within the applet expiry period. This threat model has been manageable for the traditional SmartCards as the product remains offline for most of its life and requires the card to be stolen to perform an attack. Comparing this to the Mobile world where the product will be online for most of its life, this amplifies the threat for logical attacks and thus requires the new approach as detailed in this document.

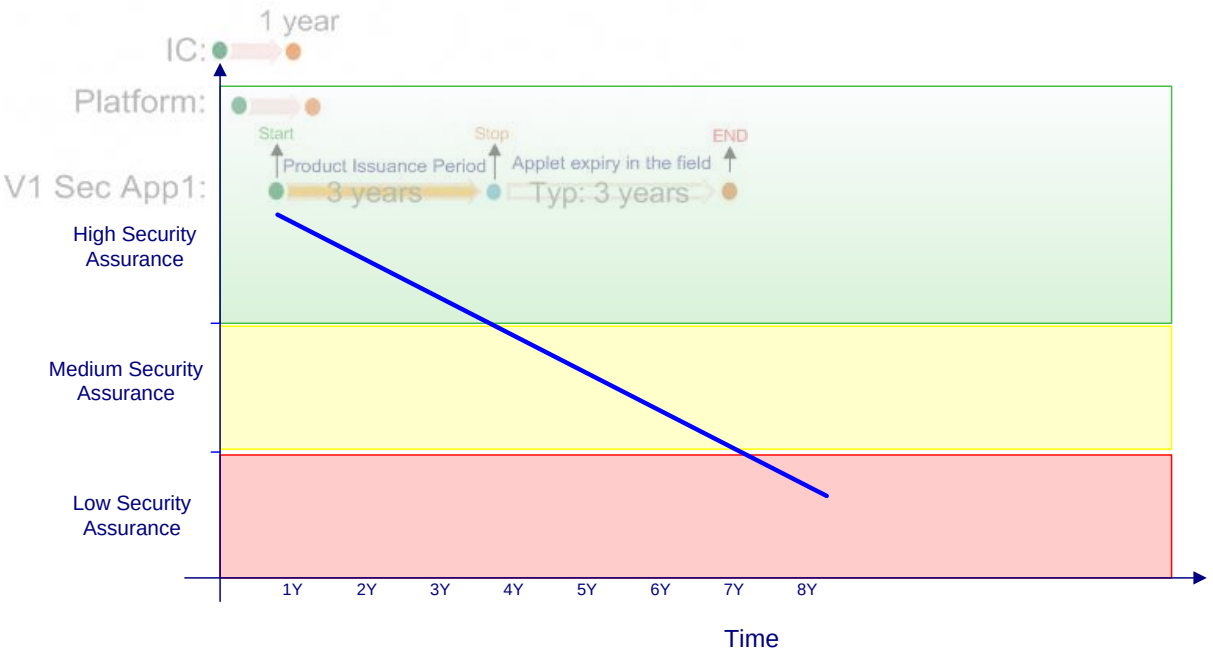


Figure 6 – SmartCard Product Security Assurance Level

When comparing Figure 5 & 6, it can be seen that the Mobile model (Figure 5) is demonstrating High assurance after 6 years, this may have been achieved with several security patches resulting in the most secure applet being delivered to the issuer / end user (device holder). When jumping across to the SmartCard model (Figure 6), after 6 years the product is likely to have slipped into Low assurance, activation of the product is not possible and the applet in the field has exceeded its personalized expiry date therefore the banking app on this product is no longer possible. Given that applet updates have not been required over the issuance period, the product may have been vulnerable to various attacks toward the end of its lifecycle.

It should be noted that Figure 5 & 6 represent a typical product and a guideline security level derived from CAST past experience. When considering the real world variety of products, the expected fall in security may be less severe or more severe than the example given. Since an accurate prediction of the fall in security over time is not possible, CAST strongly recommends a risk analysis based on fresh evaluation evidence thus providing a secure future for mobile payments.

BY GARY HEMMINGS, MASTERCARD

For more information on the CAST process please contact cast@mastercard.com