SECURE TECHNOLOGY ALLIANCE

A SECURE TECHNOLOGY ALLIANCE PAYMENTS COUNCIL WHITE PAPER

Implementation Considerations for Contactless Payment-Enabled Wearables

Version 1.0

October 2017

Secure Technology Alliance
191 Clarksville Road
Princeton Junction, NJ 08550

www.securetechnologyalliance.org

About the Secure Technology Alliance

The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption and widespread application of secure solutions, including smart cards, embedded chip technology, and related hardware and software across a variety of markets including authentication, commerce and Internet of Things (IoT).

The Secure Technology Alliance, formerly known as the Smart Card Alliance, invests heavily in education on the appropriate uses of secure technologies to enable privacy and data protection. The Secure Technology Alliance delivers on its mission through training, research, publications, industry outreach and open forums for end users and industry stakeholders in payments, mobile, healthcare, identity and access, transportation, and the IoT in the U.S. and Latin America.

For additional information, please visit www.securetechalliance.org.

Table of Contents

1 Introduction

Wearables, as a general category, cover wide variety of device types – from smartwatches to rings to wristbands to clothing – using different communications and security technologies. The total wearables market is expected to have significant growth, with a recent Gartner report estimating that 310.4 million wearable devices will be sold in 2017, growing to over 504 million by 2021.[1]

This market growth for connected devices that can be used for a variety of functions presents opportunities for device manufacturers, service providers and the payments industry. Payment-enabling wearables can make payment easier and more convenient for consumers. BI Intelligence estimates that 62 percent of wearable device shipments will include payments functionality by 2020.[2]

The Secure Technology Alliance Payments Council developed this white paper to provide a high-level overview of the landscape for payment-enabled wearables and to discuss key technology and deployment considerations for industry stakeholders. Since wearables are being developed with many form factors and technologies, the payment enablement processes can vary significantly depending on the device and technology selected. To provide concrete guidance for implementers, this white paper focuses on a subset of wearables and payment processes that encompass the most common wearables implementations today.

This white paper's scope includes:

- Wearables that support contactless transactions using technology that complies with ISO/IEC 14443
- Security based on hardware secure elements
- Provisioning models that use a broad range of technologies (e.g., WiFi, Bluetooth, over-the-wire, trusted service managers (TSMs))

Other possible wearable payment implementations that would use different technologies or business requirements are outside of the scope of the white paper; these could include in-app payment on the wearable device, geo-fencing or beacon-based authentication, and QR code implementations.

[1] "Gartner Says Worldwide Wearable Device Sales to Grow 17 Percent in 2017," Gartner news release, Aug. 24, 2017, http://www.gartner.com/newsroom/id/3790965

[2] "Here's What's Holding Back Wearable Payments," Business Insider, Mar. 10, 2017, http://www.businessinsider.com/heres-whats-holding-back-wearable-payments-2017-3

2 Payments with Wearables Defined

For the purpose of the white paper, a wearable device is defined as a small electronic device that is worn or easily carried, incorporates one or more technology-related functions, and supports contactless transactions using technology that complies with ISO/IEC 14443. Wearables may support open payment (e.g., credit and debit card payment) or closed payment (e.g., transit, event) systems.

Examples of wearable devices discussed in this white paper include: watches, rings, bracelets/wristbands, clothing, key fobs, and stickers/micro-tags. A mobile phone that has payment functionality is not considered a wearable in this document.

2.1 Wearables Hardware Technologies

Wearables are implemented with two types of hardware technologies: passive or active.

Passive wearables include a chip/secure element that has an operating system and payment app (one or more), is connected to an antenna, and has an ISO/IEC 14443 interface. Passive wearables are powered through the contactless interface. While the wearables device may have a battery to power other functions (e.g., Jawbone), it requires no battery to power payment functionality, operate the secure element or provision the device with payment credentials. Passive wearables may be stickers, key fobs, rings, or other form factors.

Active wearables include the same functionality described for passive wearables, plus another connectivity option – for example, Bluetooth or WiFi – and require a battery. The secure element has a means to connect to the rest of the world through an interface other than the ISO/IEC 14443 contactless interface.

2.2 Technology Choices and Provisioning

Payment-enabled wearables must be provisioned with the owner's payment credentials (e.g., payment account) and must be managed over the device lifecycle. This white paper reviews the following three models for active and passive devices.

- **Active connected wearable**: The active connected wearable is a powered device that requires a battery. The device connects to a mobile device and has a means to connect to a trusted service manager (TSM) for provisioning. The wearable device includes a secure element and Near Field Communication (NFC) functionality and is integrated with digital-wallet-enabled solutions (e.g., Apple Pay).
- **Passive enabled wearable**: The passive enabled wearable is based on the chip used in a traditional contactless card and is powered by the contactless reader's field. The device may require a custom antenna design to meet read/write distance requirements for the application being implemented. Independence from the mobile device (e.g., for power requirements) allows flexibility for the design. A passive enabled wearable needs to be personalized at a personalization bureau and may require custom equipment to handle different form factors.
- **Passive disabled wearable**: The passive disabled wearable is also based on the chip used in a traditional contactless card and is powered by the contactless reader's field. The device may require a custom antenna design to meet read/write distance requirements for the application being implemented. Independence from the mobile device (e.g., for power requirements) allows flexibility for the design. A passive disabled wearable needs to be personalized at the distribution channel using instant issuance personalization equipment.

Additional information on these models is covered in Section 6.

2.3 Wearable Ecosystem Stakeholders

Enabling payments in wearables involves multiple parties depending on the device type, distribution model and type of payment instrument selected for the solution.

In general, the wearable payment ecosystem includes (but is not limited to):

- Wearable device manufacturer (everything from a smart device (e.g., fitness band) to an almost disposable wearable (e.g., event wristband))
- Chip vendor
- Inlay/antenna vendor
- Card/tag/sticker/SIM vendor
- Issuing bank
- Program manager (e.g., for prepaid payment applications)
- Payment network
- Certification laboratory
- Personalization bureau
- TSM(s) (e.g., for over-the-air personalization if used)
- Tokenization service provider (TSP) (e.g., for tokenizing payment credentials)
- Wallet application and wallet service provider

3 Potential Target Applications for Payment-Enabled Wearables

3.1 Definition of "Applications"

This white paper focuses on payment applications in wearables. "Payment applications" are defined as the possible utilizations of a wearable device to perform some type of payment using the ISO/IEC 14443 contactless standard, while making use of a secure element. Such user applications correlate with secure applets that are installed in the secure element itself. Wearable devices may feature a single application or multiple applications, with many combinations possible. This section examines different applications, irrespective of how it is installed, personalized, or activated in the device; these aspects will be covered in Section 7.

In addition to payment applications, other, non-payment, contactless applications are possible, such as coupons, loyalty cards, employee badges, student ID cards, hotel room keys, and several other forms of access control and user identification. While these are considered out of scope for the white paper, they may be deployed in conjunction with the payment applications discussed in this section.

3.2 Applications

3.2.1 Debit and Credit Payment

Debit and credit payment card applications enable device owners to perform a payment at a merchant point of sale (POS) by presenting their wearable devices. The application is associated with a debit or credit card owned by the device owner. The card is associated with a deposit or credit account at a bank, credit union or other financial institution (the issuer of the card). Some form of cardholder authentication may be expected at the time of the transaction, typically signature, PIN or some other form of biometric authentication, as required by the payment networks. Credit and debit card payment transactions may also allow no cardholder verification method (No CVM), if the transaction meets certain parameters set by the payment networks. The payment card application on the wearable device may represent cards transacting on any of the payment networks (such as American Express, Discover, Mastercard, Visa, Maestro, Cirrus or others), each of which has its own corresponding applet in the secure element.

3.2.2 Private Label Payment

Private label payment cards may be issued by financial institutions or merchants. With merchant private label cards, the merchant acts as the issuer of the card to the end user, who may have an account with the merchant or a financial institution appointed by the merchant. The account may be funded with credit accounts or linked to a bank account. Private label payment card applications enable users to link their physical cards or accounts to a matching application on the wearable device.

Similar to credit or debit card applications described in the previous section, private label payment applications enable device owners to present their wearable device at a POS to perform a transaction. Unlike the previous category that represents cards transacting on payment networks, private label payment cards may transact on a "closed loop" network which is merchant specific.

3.2.3 Prepaid Payment

Prepaid payment cards have emerged as popular methods of cash management. Prepaid cards are most often purchased by customers at retail locations. Customers must load funds onto their cards in advance, which can be done either electronically or in-store. These cards are generally subject to little governance, and most issuers do not require cardholder verification methods.

This category includes gift cards, which can be regarded as a prepaid version of a merchant card. Gift cards can only transact at a specific merchant location.

Another type of card is the general purpose reloadable (GPR) card. GPR cards are generally associated with a payment network (e.g., American Express, Discover, Mastercard, Visa) and can be used to make purchases wherever credit or debit cards are accepted. Most companies charge the cardholder fees to reload funds or to make purchases through PIN debit or signature methods.

3.2.4 Event Pass

Event pass and season pass ticketing applications allow users to redeem access to venues for which the ticket is valid (e.g., concerts, sporting events). The event access credential is stored in an applet in the secure element and presented at a contactless access control gate of some sort. The application can also be extended to other types of "events" (e.g., VIP passes or theme park access). In this case, the access credential can be linked to a funded account associated with the user, to allow the user to use the same ticketing application to purchase additional services at the venue (such as food, drinks, souvenirs) within a closed loop ecosystem. Specially enabled contactless terminals are placed at the point of transactions within the venue, such as at restaurant kiosks or merchandise stores.

3.2.5 Transit

The modern public transit infrastructure often relies on contactless technology for fare media and access control; notable examples are Chicago Transit Authority Ventra and London Oyster cards, which rely on ISO/IEC 14443. Transit ticketing applications are possible applications for wearable devices equipped with a secure element, where the ticket credential will be stored. Single ride tickets are valid for a single use; account-based tickets allow users to ride multiple times as long as the account is funded; monthly or multi-trips are valid for a certain period, with value subtracted from the stored value for each trip.

The method for reloading funds can vary by deployment and the user interface capability allowed by the device; however, the versatility of a wearable device equipped with a secure element is uniquely positioned to offer the high security and fast transaction speed required by transit applications.

4 Benefits of Payment-Enabled Wearables

Using wearable devices for payment is an idea that's been sought after for years. Over 10 years ago, the payment industry introduced payment stickers as a universal alternative payment form factor. Payment now encompasses many complimentary form factors, including stickers and a wide variety of wearables.

This section summarizes key benefits of payment-enabled wearables for consumers, issuers, merchants, prepaid program managers/event organizers, and OEMs/device manufacturers.

4.1 Consumers

Wearable devices present a unique advantage for end users when embodying the applications discussed in Section 3. The wearable device is always with the user, therefore less subject to loss. It is ready for use at the time of redemption. Convenience is a primary value proposition for the end user.

Wearable devices simplify a user's daily activity, which is especially beneficial for those activities with repeat use. Payment-enabled wearables best fulfill their purpose when other forms of payment are not available or are less convenient to use. Examples include: paying with a wearable for a refreshment or snack at an event where a purse or wallet isn't otherwise necessary; buying a quick coffee or daily groceries; paying for transit system access. All of these daily consumer activities are made more convenient with a wearable device like a wristband or a ring.

4.2 Issuers

Wearables benefit issuers by enhancing the frequency of use of a payment credential by providing consumers with a new and convenient form of payment. Wearables offer a significant benefit to the issuer since, much like bank-issued cards, wearables can carry branding. A branded wristband used for payment and access can provide significant marketing benefits to an issuer. Compared to cards that consumers keep in their wallets, a branded wearable device that's worn on the wrist remains top-of-mind – not just top-of-wallet – and is visible to others around the consumer wearing the device.

4.3 Merchants

Frequency and convenience are key drivers to increase sales and consumer loyalty. Merchants can increase loyalty by offering wearable devices that are convenient to use. Wearables can be co-branded with a financial institution and leverage the benefits of marketing and loyalty comparable to those of the financial institution partners. Merchants may also introduce product branding opportunities via sponsorships and promotions.

An additional wearables use case for merchants and issuers is to build consumer-engagement programs combined with quality of living and products/services being offered. For example, fitness tracking and nutrition or activities rewards programs can be consolidated into a wearable's functionality along with payment.

4.4 Prepaid Program Managers/Event Organizers

Program managers are a category of issuing entities that can work in partnership with financial institutions to drive cashless consumer payment experiences in single or season-long events or environments. Payment functionality can be combined with access control and ticketing to create a single device that delivers consumer-friendly, one-stop engagement. This can also drive consumer "stickiness" through fan loyalty, while using the device beyond the designated environment. This use case can further extend the life of the wearable and the use of the prepaid account.

4.5 Device Manufacturers/OEMs

Consumer-centric device manufacturers continually explore new desired features. Payment functionality has been a central focus for feature innovation for all of the major mobile handset manufacturers, and payment technology is now being propagated into wearable devices. Watches, fitness trackers and other connected devices compete for consumer preference. Payment functionality is proving to be of importance when consumers choose one device over another. In addition, new cross-functional experiences can be offered to the consumer by building in new use cases: for example, fitness bands with financial rewards. Wearable device manufacturers do not need to become experts in payment technology to implement payment functionality. Payment technology suppliers already offer white-label wearable payment solutions that can be easily integrated into an existing hardware and software wearable platform.

5 Current Examples of Payment-Enabled Wearables

Much like the world of the Internet of Things (IoT), the number of wearables may be limited only by one's imagination for what consumers would want to wear and have enabled for payment -- from accessories such as watches and jewelry, to garment attachments, eye wear, hats and more. Given the breadth of options for wearables, it is important to understand the functional and connectivity capability built into active and passive wearables.

5.1 Active Connected Wearables

Active connected wearables can accept, produce or communicate dynamic content to the consumer and/or another device. Such wearables have both an ISO/IEC 14443 interface and another communications interface and have their own power source. These devices most often will have a Bluetooth or other wireless communication interface and are paired to a mobile device or communicate directly to the Internet via WiFi or cellular connectivity.

Active connected wearables are provisioned with payment credentials in real-time while facilitating additional functionality such as an information display to deliver content to consumers – either self-generated content (e.g., fitness tracking, geolocation) or over-the-air dynamic content.

Examples of active connected wearables include: powered watches with Android, Apple or other proprietary operating systems; fitness/activity/health trackers; special purpose devices such as location trackers. All active, connected wearables may be combined with payment functionality.

5.2 Passive Wearables

For payment-enabled functionality, passive wearables have no additional means for information delivery or communications, and rely entirely on the ISO/IEC 14443-enabled contactless interface to function. Passive devices do not have a power source of their own. Passive wearables may be provided to the consumer with a generic (prepaid) credential already loaded and activated and associated with the consumer before first use.

The technology available today does not limit passive wearables to be pre-enabled with payment credentials. Similar to traditional payment cards, passive wearables may be instantly issued in the field leveraging the contactless interface.

Examples of passive wearables are: wristbands; rings; universal "insertable" devices, like a SIM-sized card or other card break-out piece which can be inserted into multiple end-form factors (for example with different forms of bands, band attachments or other accessories). Fully pre-assembled wristbands and wristbands with insertable card break-out pieces have their own advantages and disadvantages depending on the use case and application.

6 Differences in Wearable Payments Implementations

For the purpose of this white paper, three models for payment-enabled wearables are considered:

- Passive enabled wearables that are pre-personalized
- Passive disabled wearables that must be personalized in the distribution channel
- Active connected wearables that are provisioned over the air

As described in Section 5, one of the main differences between passive and active wearables is the type of interfaces to/from the secure element. This interface determines implementation differences for personalizing the wearable with payment credentials used by the user.

6.1 Passive Enabled Wearables – Pre-personalized

Passive wearables typically rely on the ISO/IEC 14443 contactless interface as the only means of communications. Bulk issuance of such devices requires that secure elements be deployed with pre-installed, pre-personalized applications prior to delivery to the distribution or retail channel. (This is referred to as a "static" configuration.) These devices are delivered to customers fully personalized with payment credentials provisioned to the secure element at the time of manufacturing, prior to issuance; the payment credentials cannot be changed in the field.

When the end device is associated with a user, the credential can be activated in the issuer's back-end system and thus associated with the specific user. Suitable application examples for this type of implementation are prepaid cards (such as general purpose reloadable cards) or closed loop card applications (such as event ticketing). Credit and debit card applications may also be suitable, but may require tokenization. (See Section 7.2.2 for additional information on tokenization.).

6.2 Passive Disabled Wearables – Instantly issued

While the activation of passive wearables via the back-end system allows users to perform the activation remotely, certain deployments benefit from activation taking place at a physical location, such as at a retail store, at a bank branch, or at an event or theme park. For these deployments, user identity can be verified and the wearable device becomes an integral part of the brand experience.

An on-site method of passive device personalization is possible leveraging the ISO/IEC 14443 interface. In this case, rather than pre-installing a credential at manufacturing, the personalization can happen post-issuance, via a proximity mechanism that has been approved by the issuer or service provider (e.g., at a kiosk or bank branch). In this case, the contactless reader loads the credential to the secure element. Personalization at point of delivery is often referred to as "instant issuance." All types of payment applications are suitable for this implementation. These implementations tend to be issuer specific, in that the contactless reader needs to authenticate the secure element. Implementations can easily include credit and debit cards, where instant provisioning would be done at a bank branch equipped with readers capable of issuing a new primary account number (PAN), or a tokenized variant associated with an existing account.

6.3 Active Wearables – Over-The-Air Provisioned

Active wearables can accept, produce or communicate dynamic content to the consumer and/or another device. Payment applications can be loaded and personalized in the field, as these devices are typically connected via Bluetooth Low Energy (BLE) or WiFi to a companion mobile device for over-the-air provisioning in tethered mode; active wearables may also have cellular connectivity of their own for

untethered operation. To allow for real-time, over-the-air provisioning of payment credentials and other dynamic content, the secure elements used in these applications must have additional interfaces besides those required for contactless operation and must operate in full mobile configuration. The dynamic creation of security domains, the installation of applets, and the personalization of applets require that a wallet-like application be present, either on the wearable device, on the companion mobile device, or on both.

To ensure overall solution security, implementations must adhere to agreed-upon robust standards, such as GlobalPlatform.[3] Issuers, payment networks, device manufacturers, and secure element vendors must work closely to ensure the interoperability of provisioning systems and methods and to ensure that payment applications work as intended in the field. Stakeholders such as device manufacturers, issuers, payment networks and event organizers will face a make-or-buy decision for deployments, and will often look to specialized vendors to source proven solutions and meet time-to-market requirements. From wallet platform vendors to token service requestors to token service providers to turnkey platform and services vendors, service providers are emerging to provide certified platforms to enable and simplify deployments for these stakeholders.

[3] http://www.globalplatforum.org

7 Payment Enablement and Deployment Considerations

Payment enablement solutions are divided into two main groups according to the purpose of use: closed loop and open loop payment.

In **closed loop solutions**, wearable devices can only be used on specific readers and for specific applications after being personalized. Prepaid tickets in transportation, loyalty cards and concert tickets are some examples of closed loop applications. With **open loop payment solutions**, regardless of the purpose of use or reader type, the wearable can be used with all contactless EMV-capable readers (as with contactless credit or debit cards).

To enable a wearable as a payment device, some steps need to be done according to the wearable device type.

7.1 Eligibility Checks

Before enabling an active or passive wearable device as a payment instrument, a critical step is checking whether the wearable device is eligible for use with payments and if the customer is eligible to own the payment card. If the device is eligible to use and the customer is eligible to own the card, then the system can provision a payment credential to the wearable. These controls are required for solutions where active wearable devices are used.

7.2 Provisioning

The provisioning step is when card credentials are downloaded to the wearable device so that they can be processed by the issuer of the card or a third-party stakeholder on behalf of the issuer. In the solutions where "active connected" devices are used, the provisioning process can be completed at any time and any place according to the customer's needs. "Passive disabled" or "passive enabled" devices can be provisioned before delivery or at point of delivery as mentioned in the previous sections.

In wearables with secure elements, payment card credentials in "passive enabled" and "passive disabled" devices are as safe as in the chip cards with which consumers are familiar. Therefore, the steps to verify cardholder identity or provision card credentials are similar to traditional credit and debit chip cards. However, with "active wearable" devices, a mobile phone or other device is needed to assist in managing the device or provisioning a card. **Figure 1** depicts how a mobile phone assists a cloud-based service in managing the wearable device.

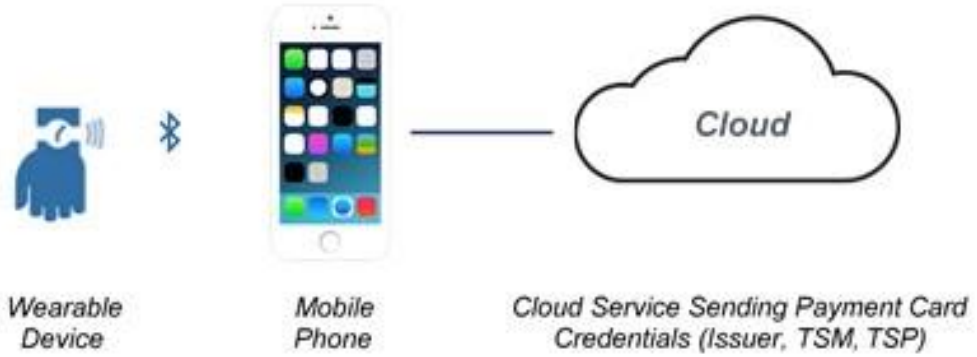

Figure 1. Mobile Phone Assisted Provisioning of Wearable Device

In the solutions where "active wearable" devices are used, the following topics should be considered:

1. Cardholder verification during use: If the wearable device is provisioned as a closed loop card, such as a transit or loyalty card, it may not be important to verify the cardholder identity. If it is an open loop payment card, such as a credit or debit card, then the appropriate cardholder verification method should be used.
2. Secure communication between the mobile phone and the cloud: Card credentials should be protected during and after transmission from the cloud service.
3. Devices connecting to an individual's wearable: The wearable and the mobile device are connected to each other via Bluetooth. The connection between the wearable and the mobile device must be limited to the owner's device and prevent other mobile devices from connecting to an individual's wearable.
4. Black list control: Users that have made some unauthorized transactions should be restricted when downloading card credentials or using the wearable devices.

7.2.1 Alternative Methods for Provisioning to a Secure Element

Access to a secure element is controlled in order to reduce or eliminate the risk of compromising payment credentials; therefore, only authorized parties are allowed to "unlock" a secure element so that it can be loaded with the payment credential.

In a "traditional" model, a Secure Element Issuer Trusted Service Manager (SEI TSM) would manage access and enable provisioning of a token into the secure element. Integration of the SEI TSM and Service Provider TSM (SP TSM) can be challenging. The methods and techniques can vary from vendor to vendor, making it harder to manage content across multiple secure elements. That adds time and complexity to the development cycle, increases operating costs, and raises overall risk.

Different models are emerging to simplify provisioning to a secure element.

Recently a new model – the Secure Element Management Service (SEMS) SCP11c secure channel protocol (DSEM)) – has been developed to simplify the provisioning process. This new secure channel protocol, included in GlobalPlatform Amendment A, facilitates generation of static 'scripts' that can be executed on a group of secure elements by directly addressing the application provider's security domain.

The SEMS certificate authority (CA) delegates content management rights using certificates. Application providers will be issued certificates, that include content management rights, which can be used to establish a secure channel with the secure element. Applets can be loaded on a large scale, without using an SEI TSM. SEMS SCP11c-based scripts are either preloaded in the wallet application or sent from the wallet platform, and can trigger various card content-management operations. For example, the scripts can create security domains and inject keys, load and update applets, instantiate applets, delete security domains, and delete applets. The same SEMS SCP11c-based scripts enabling content-management operations can be used across multiple devices from one device provider or even from multiple device providers, greatly lowering the complexity of managing secure-element-based services and related costs and enabling extremely fast time-to-market.

SEMS coexists with the SEI-TSM-based model, yet represents a plug-in replacement for the conventional SEI-TSM approach. Since SEMS SCP11c/DSEM uses just one real-time connection, it reduces system testing and minimizes the risk of failure. SEMS also offers the highest level of data protection and encryption, and produces a fully EMV-certified system that can be used anywhere in the world.

SEMS SCP11c is undergoing standardization at GlobalPlatform (GP) in the form a new existing GP Amendment A.

7.2.2 Tokenization

Tokenization is defined as the replacement of a high-value credential (e.g., PAN) with a surrogate number that can only be used within a particular context. Payment tokens are now being used in multiple payment channels, including with NFC-enabled mobile payments and in payment-enabled wearables.

A new role in the payment ecosystem is needed to support tokenization, called the Token Service Provider (TSP). Payment tokens are generated by a TSP, which may be the card issuer or a third party on behalf of the issuer. Today, tokenization services are generally offered by global or domestic payment networks. Examples are: Mastercard Digital Enablement Services (MDES); Visa Token Service (VTS); Discover Digital Exchange (DDX); Interac (domestic TSP for Canada).

For payment-enabled wearables, tokens represent the PAN and every wearable device should be associated with a token (either short-lived or long-lived depending on the issuer and the use case).

The token requester is the entity that requests that the TSP issue a token. This entity may be a merchant, a wallet provider, an issuer or another party.

A general token deployment process is illustrated in Figure 2. The token requester initiates the process and requests that the TSP generate a token. The TSP performs an identification and verification (ID&V) process and asks the issuer for authorization to generate a token. The TSP generates the token and returns it to the token requester. The token requester securely provisions the token into the wearable device.

Figure 2. Token Deployment Process

8 Lifecycle Management

The specific manufacturing and distribution models, as well as the day-to-day usage, of wearable devices represent a significant change for lifecycle management compared to other payment devices.

Device manufacturers and service providers need to be aware that even after the payment credential has been provisioned and device has been delivered to end user, there is still a need to manage the lifecycle of the credential and the wearable itself. This section summarizes some of the key considerations in lifecycle management.

8.1 Re-provisioning or Adding Value

Wearables may need to be re-provisioned or allow value to be added (for open or closed loop prepaid applications). Wearable devices can change user ownership; while an active device would likely follow the same process as mobile devices, passive devices represent a completely different challenge as a device needs to be unlinked and the functionality might be completely disabled after the device changes owners.

Implementing this functionality may include interaction with companion applications or integration of third party APIs and digital wallets. Re-provisioning rules also need to be defined in case the wearable needs to be replaced or fixed due to failure of non-payment functionality.

8.2 Expiration of Payment Credentials

For wearable devices, the payment credential expiration may be defined by the actual type of device. Some disposable or semi-disposable wearable devices may use a traditional card model, while high-end passive devices (e.g., fitness wearables) may have different expiration rules.

8.3 Deactivation of Payment Functionality

Payment functionality in a wearable device should be able to be temporarily or permanently disabled (for example, if a user loses, sells or disposes of the wearable device).

8.4 Payment Enablement after Wearable Deployment

Due to wearable distribution models, the device manufacturer along with the issuer and payment network need to define how the payment credential is activated after the wearable is purchased by the consumer. While this should be simple for active wearables due to the established mobile device provisioning model, passive devices could, in theory, have a fully personalized payment credential, requiring an activation process that associates an anonymous credential to a consumer account.

8.5 Consumer Choice of Payment Method on Passive Wearable Device

Beyond low-end, event-specific wearables, industry stakeholders should have limited or no expectations of a cardholder owning multiple wearables, each with a different payment credential. Active devices address this through digital wallets. Passive devices need to rely on third-party services if there is a need to link accounts via proxy cards or by linking multiple accounts to fund prepaid products.

9 Certifications, Approvals, Branding and Interoperability Requirements

Depending on the technology chosen, the payment networks may have defined guidelines for wearables implementing open loop payments. Considerations include:

- Testing and certification of physical characteristics, contactless interface performance and payment functionality
- Interoperability testing
- Graphics or branding required on the wearable
- Requirements for wearables as health-related devices

For open loop payment, the testing and certification process is similar to the one used for cards and NFC-enabled mobile devices; however, some functionality and specifications may be different. Issuers should consult with the payment networks for the required testing and certification processes and guidelines.

For closed loop payment, the testing and certification process depends on the use case and readers in place, and will be driven by the infrastructure being deployed or already in use. Testing and certification requirements would be specified by the organization issuing the wearable (e.g., transit agency, event organizer).

During the testing and certification process, device interoperability will be tested with terminal read range one measure that is tested.

In addition to payment networks' branding and functional/interoperability certifications and approvals, it is recommended that the device manufacturer identify any regional requirements for specific testing needed for health-related wearables. For example, for wearable payment devices that are intended to be in continuous contact with the human skin, the following ISO standards may apply:

- ISO 10993-10: Biological Evaluation of Medical Devices – Part 10: Tests for irritation and skin sensitization
- ISO 10993-12: Biological Evaluation of Medical Devices – Part 12: Sample preparation and reference materials

10 Conclusions

The payment-enabled wearables market is emerging and expected to show significant growth. A variety of form factors and technologies are being used, with the choice of technology having a significant impact on the models for provisioning and managing the lifecycle of the wearable device.

When implementing payment-enabled wearables, industry stakeholders should consider the following:

- How will the consumer be motivated to use the wearable for payment? Will there be sufficient acceptance points?
- What is the use case for the wearable? Who is the target customer and when, how and where is the wearable going to be used? Understanding the use case will help with the technology decisions.
- Who are the stakeholders that will be involved in manufacturing, provisioning, distributing and managing the wearable device? The stakeholders outlined in Section 1 have different roles depending on the application use case and technology model selected.
- What is the certification, testing and approval process? How does this process fit with the overall timeline required for the wearable project?
- How will the payment-enabled wearable lifecycle be managed? Identification of the industry partners needed to provision and manage the wearable during its lifecycle is critical.

Payment-enabled wearables offer new opportunities for wearable device manufacturers, service providers and the payments industry to offer consumers exciting new payment form factors. From improved convenience for consumers to increased loyalty and “brand stickiness” sought by device manufacturers and service providers, wearables deliver benefits to all stakeholders in the ecosystem.

11 Publication Acknowledgements

This white paper was developed by the Secure Technology Alliance Payments Council to provide an educational resource on the wearables landscape focusing on ISO/IEC 14443/secure element-based implementations and to discuss key considerations for implementing payments in wearables.

Publication of this document by the Secure Technology Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Secure Technology Alliance wishes to thank Council members for their contributions. Participants involved in the development and review of this white paper included: American Express; Cardtek US; Discover Financial Services; G+D Mobile Security; Gemalto; GlobalPlatform; IDEMIA; Infineon Technologies; IQ Devices; Mastercard; Metropolitan Transportation Authority (MTA); Multos International; NXP Semiconductors.

The Secure Technology Alliance thanks Council members who participated in the project team to write and review the document, including:

- **Philip Andreae**, IDEMIA
- **Stefania Boiocchi**, Infineon Technologies
- **Hank Chavers**, GlobalPlatform
- **Jose Correa**, NXP Semiconductors
- **Brady Cullimore**, American Express
- **Jack DeLangavant**, Multos International
- **Melanie Gluck**, Mastercard
- **Murat Guzel**, Cardtek US
- **Jack Jania**, Gemalto
- **Kenny Lage,** Discover Financial Services
- **Joshua Martiesian**, MTA
- **Cathy Medich**, Secure Technology Alliance
- **Sadiq Mohammed**, Mastercard
- **Nick Pisarev**, G+D Mobile Security
- **Steve Rogers**, IQ Devices
- **Fatih Teksoy**, Cardtek US
- **Erdal Yazmaci**, Cardtek US

Trademark Notice

Legal Notice

About the Secure Technology Alliance Payments Council

The Secure Technology Alliance Payments Council focuses on securing payments and payment applications in the U.S. through industry dialogue, commentary on standards and specifications, technical guidance and educational programs, for consumers, merchants, issuers, acquirers, processors, payment networks, government regulators, mobile providers, industry suppliers and other industry stakeholders.

The Council's primary goal is to inform and educate the market about the means of improving the security of the payments infrastructure and enhancing the payments experience. The group brings together payments industry stakeholders to work on projects related to implementing secured payments across all payment channels and payment technologies. The Payments Council's projects include research projects, white papers, industry commentary, case studies, web seminars, workshops and other educational resources.

Additional information on the Payments Council can be found at https://www.securetechalliance.org/activities-councils-payments/.